UNIVERSIDAD DE CUENCA

Facultad de Ingeniería

Carrera de Ingeniería de Sistemas

Metodología para la recolección de evidencia forense generada durante la utilización de aplicaciones desplegadas en entornos web.

Trabajo de titulación previo a la obtención
del título de Ingeniero en Sistemas

Autor:

Bryan Daniel Coronel Tapia
CI: 0105682082

Directora:

Ing. Karina Pamela Campus Argudo, MSc
CI: 0103143830

Co-Directora:

Ing. Irene Priscila Cedillo Orellana, PhD

CI: 0102815842

Cuenca - Ecuador

2018

Resumen

En la actualidad, con el creciente uso de aplicaciones web también se ha incrementado el índice de problemas y crímenes a través de aplicaciones web, por lo que surge la necesidad de una guía que contemple técnicas forenses digitales para el manejo de evidencia digital proveniente de entornos web. El problema principal al interactuar con aplicaciones web es conocer exactamente donde se encuentra la información o si es posible acceder a la misma por la jurisdicción geográfica; en consecuencia, una alternativa viable para poder realizar un adecuado peritaje informático es llevar a cabo la investigación en el ordenador (lado del cliente). Si bien existen metodologías y casos de estudio que brindan guías y buenas prácticas, la gran mayoría están enfocadas para aplicaciones web específicas; es decir, no pueden ser generalizadas para contemplar cualquier posible situación.

El presente trabajo de titulación presenta una revisión de literatura de las tendencias y prácticas en esta área de estudio y propone una metodología que permita a los investigadores forenses llevar a cabo una investigación hasta el cierre de la misma. Para la elaboración de la metodología además de considerar guías y buenas prácticas de expertos, se ha hecho uso de recomendaciones provistas por estándares internacionales, a la vez que se implementó una herramienta que permite disminuir los tiempos de recolección de los principales artefactos provenientes de interacciones con entornos web, garantizando la integridad de los datos recolectados.

Palabras clave: Evidencia digital, Informática forense, Arquitectura Cliente-Servidor, Entornos Web, Caché, Cookies.

Abstract

Nowadays, with the increasing on the use of web applications, the rate of problems and crimes through them has also increased. Therefore, that is the reason for the need of a guide that includes digital forensic techniques manage digital evidence from web environments. The main problem, when users are interacting with web applications, is to know exactly where the information is located, or if is possible to access it because of the geographic jurisdiction; consequently, a viable alternative to perform an adequate computer expertise is to carry out the investigation on the computer (client's side). However, while there are methodologies and case studies that provide guidance and good practices, the majority are focused on specific web applications; that is, they cannot be generalized to cover every possible situation.

This investigation presents a literature review of trends and practices in this area of study and proposes a methodology that will enable forensic investigators to conduct an investigation throughout the end of it. For the development of the methodology, in addition to considering guidelines and good practices from experts, emphasis has also been placed on recommendations provided by international standards, also a tool has been implemented to reduce the collection times of the main artefacts coming from interactions with web environments, guaranteeing the integrity of the data collected. At the end, the proposals of this study are evaluated by means of a test of concepts.

Keywords: Digital Evidence, Forensic Computing, Client-Server Architecture, Web Environments, Cache, Cookies.

Índice de Contenidos

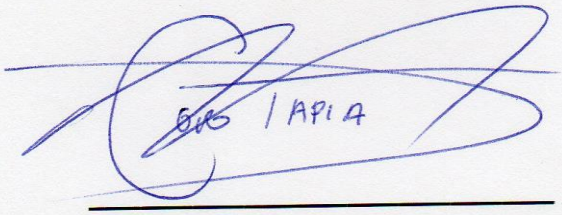
Lista de Tablas

Lista de Figuras

Cláusula de Propiedad Intelectual

Yo, Bryan Daniel Coronel Tapia, autor del trabajo de titulación "Metodología para la recolección de evidencia forense generada durante la utilización de aplicaciones desplegadas en entornos web", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 22 de octubre de 2018



Bryan Daniel Coronel Tapia

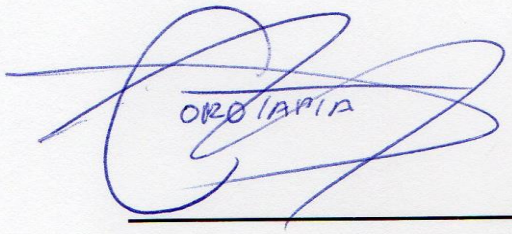
C.I: 0105682082

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

Yo, Bryan Daniel Coronel Tapia en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación "Metodología para la recolección de evidencia forense generada durante la utilización de aplicaciones desplegadas en entornos web", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 22 de octubre de 2018



Bryan Daniel Coronel Tapia

CI: 0105682082

Lista de Abreviaciones

API	Interfaz de Programación de Aplicaciones (*Application Programming Interface*)
ARP	Protocolo de Resolución de Direcciones
COIP	Código Orgánico Integral Penal
FaaS	Forense como Servicio *(Forensic as a Service)*
HTTP	Protocolo de Transferencia de Hipertexto *(Hypertext Transfer Protocol)*
IaaS	Infraestructura como Servicio *(Infrastructure as a Service)*
IEC	Comisión Electrotécnica Internacional
IP	Protocolo de Internet *(Internet Protocol)*
ISO	Organización Internacional para la Estandarización
JPEG	Grupo Conjunto de Expertos en Fotografía *(Joint Photographic Experts Group)*
MAC	Código de Autenticación de Mensaje *(Message Authentication Code)*
NIST	Instituto nacional de Estándares y Tecnología *(National Institute od Standards and Technology)*
PaaS	Plataforma como Servicio *(Platform as a Service)*
PNG	Gráficos de Red Portátiles *(Portable Network Graphics)*

RAM	Memoria de Acceso Aleatorio *(Random Access Memory)*
REST	Transferencia del Estado de Representación (Representational State Transfer)
RFC	Solicitud de Comentarios *(Request form Comments)*
RSS	Sindicación Realmente Simple Really Simple Syndication
SaaS	Software como Servicio *(Software as a Service)*
SPEM	Metamodelo de Ingeniería de Procesos de Software *(Software Process Engineering Metamodel)*
SOA	Arquitectura Orientada a Servicios
SOAP	Protocolo Simple de Acceso a Objetos *(Simple Object Access Protocol)*
TCP	Protocolo de Control de Transmisión *(Transmission Control Protocol)*
TI	Tecnologías de la Información
UDDI	Descripción, Descubrimiento e Integración Universales *(Universal Description, Discovery and Integration)*
URI	Identificador de Recursos Uniforme *(Unirform Resource Identifier)*
URL	Localizador Uniforme de Recursos
XML	Lenguaje de Marcado Extensible *(Extensible Markup Language)*

Agradecimientos

Agradezco a todos y cada uno de los docentes que tuve la dicha de tener en cada uno de los semestres, pues todos me guiaron con conocimientos que fueron de mucha ayuda para este trabajo de titulación. De manera particular quiero también agradecer a:

A las ingenieras Karina Campos y Priscila Cedillo, directora y codirectora de tesis respectivamente, por sus valiosas guías y el tiempo brindado para la realización de este trabajo de titulación.

De igual manera a la ingeniera Alexandra Bermeo, quien aporto en correcciones valiosas para las publicaciones generadas en la realización de este trabajo.

Al Ing. Esteban Mora, por permitirme ejecutar la evaluación del objetivo de este trabajo en una de sus sesiones de clases.

Gracias a todas las personas que ayudaron directa e indirectamente a la realización de este trabajo de titulación.

Dedicatoria

Este trabajo es la conclusión de años de esfuerzo y trabajo. Por lo que dedico el mismo:

A mi madre y mi padre, que siempre estuvieron conmigo y me han apoyado durante todo este periodo universitario tanto en momentos positivos como negativos. Este trabajo no lo podría haber logrado sin su inspiración.

A mi hermano, quien con su ejemplo me dio una visión diferente de la vida que contribuyo a mi formación.

A las directoras del presente trabajo de titulación, por estar pendientes y disponibles cuando requerí su ayuda.

A mi compañera de vida incondicional Leslee, que me ha apoyado en todas las decisiones que he tomado y me ha motivado para culminar este trabajo de titulación.

A todos mis amigos del “Team Sistemas”, por brindarme su valiosa amistad y motivarme a cumplir todos mis objetivos. Espero de corazón puedan cumplir los suyos.

Capítulo 1: Introducción

El presente capítulo brinda al lector una idea exacta de los diversos aspectos que componen el presente trabajo de investigación; detallando, su motivación, objetivos, tareas de investigación y la estructura de trabajo del trabajo de investigación.

1.1. Motivación

El Internet ha creado un mundo interconectado, a través del cual, es posible intercambiar información de forma sencilla en casi todas las ubicaciones geográficas; este hecho, ha generado el desarrollo de aplicaciones web basadas en diversos paradigmas como SOA (Arquitectura Orientada a Servicios) o la computación en la nube. Esto ha permitido un cambio en la forma en que se utiliza y consume los recursos de TI, con su aceptación tanto en entornos públicos como privados, permitiendo crear aplicaciones más usables en entornos web (Benslimane, Dustdar, y Sheth, 2008; Galante y Bona, 2012; Ricca y Tonella, 2001).

Las aplicaciones desplegadas en entornos web proveen, entre otros, servicios de comunicación, almacenamiento o comercio electrónico; y ante su creciente adopción por los usuarios finales o clientes, también se han incrementado los crímenes en la web; de ahí, surge la necesidad de un conjunto de métodos que permitan obtener evidencia generada por la interacción y las acciones realizadas en el uso de estas aplicaciones a través de técnicas forenses, con el fin de esclarecer situaciones críticas sobre su utilización en caso de ser requerido. Por otra parte, los obstáculos para realizar un análisis forense son muy comunes debido a los desafíos por las particularidades de los proveedores de servicios de hospedaje de la información (Bakshi, 2009; Galante y Bona, 2012; Lewis, 2013; Li, Tang, Hu, y Chen, 2015; Ricca y Tonella, 2001; Ruan, Carthy, Kechadi, y Baggili, 2013).

El reto principal al que se enfrentan los investigadores en aplicaciones web, en la arquitectura más común cliente-servidor, donde el cliente es el sistema o programa que solicita tareas específicas al servidor (Held, 2000), es que gran parte de las buenas prácticas y guías dentro del análisis forense en entornos web, están enfocadas en su mayoría del lado del servidor, surgiendo otra problemática acerca de la ubicación de la información (Chen, Xu, Yuan, y Shashidhar, 2015; Simou, Kalloniatis, Kavakli, y Gritzalis, 2014) . Puesto que en aplicaciones que alojan sus datos en la nube o en un servidor desconocido; la identificación, recolección y organización de la evidencia, en gran medida, depende del proveedor del servicio (Sang, 2013; Zawoad y Hasan, 2016). Los

desafíos por conocer en dónde se ubican exactamente los datos, ya que éstos pueden estar distribuidos geográficamente en diferentes lugares y para obtener dicha información existe dependencia de la jurisdicción y normativas de cada una de las localidades (Morioka y Sharbaf, 2016). Por este motivo, se realizan solicitudes a los proveedores para obtener dicha información; sin embargo, esto puede generar problemas al momento de garantizar la integridad de dicha información o una correcta cadena de custodia para que la evidencia pueda ser útil en una investigación judicial (Choo, Esposito, y Castiglione, 2017). Debido a estas dificultades nace la necesidad de brindar soluciones del lado del cliente, en donde la investigación puede ser ejecutada sin las limitaciones mencionadas (Zawoad y Hasan, 2016). Pese a la existencia de varios estudios dirigidos a la adquisición de evidencia digital, proveniente de entornos web (Majeed, Zia, Imran, y Saleem, 2015; Oh, Lee, y Lee, 2011; Oh et al., 2011; Ohana y Shashidhar, 2013) se ve la ausencia de una metodología íntegra, que permita a un investigador cubrir etapas importantes de una investigación forense como la identificación de la evidencia web, recolección, preservación, análisis y presentación de la misma de acuerdo a la ISO/IEC 27037 (2012): Directrices para identificación, recolección, adquisición y preservación de evidencia digital (Guidelines for identification, collection, acquisition and preservation of digital evidence).

Bajo este contexto y motivación, el presente trabajo de titulación propone la creación de una metodología completa, que permita: (i) identificar, (ii) recopilar, (iii) preservar y (iv) presentar evidencia digital proveniente del ordenador del lado del cliente. Esto ayuda en la identificación de actividades o interacciones de usuarios con aplicaciones o servidores desplegados en entornos web. Con el fin de probar la factibilidad de esta propuesta, se analizarán acciones de usuario en sitios tales como: Dropbox, Drive de Google o One Drive, que permiten cargar, descargar, eliminar y modificar archivos en un servidor desconocido desde aplicaciones de uso frecuente, por usuarios o aplicaciones comunes como por ejemplo navegadores. Puesto que según Morioka y Sharbaf (2016), en el ordenador local pueden existir rastros de esta interacción en cachés, cookies de navegación, archivos temporales, logs o si se tiene la posibilidad de capturar el tráfico de la red se pueden recuperar fragmentos de información de la interacción entre el ordenador y mencionadas aplicaciones web.

1.2. Objetivos

Este trabajo tiene como objetivo general, definir una metodología para realizar un análisis forense de la evidencia digital del ordenador en el lado del cliente, proveniente del uso de aplicaciones y recursos de software desplegados en entornos web (análisis de la última huella).

Como objetivos específicos que ayudarán durante la consecución del objetivo general se ha considerado:

- Realizar un estudio del estado actual de la investigación, en cuanto a la identificación, recolección, preservación, análisis y presentación de la evidencia digital proveniente de entornos web orientados al aprovisionamiento de servicios.
- Proponer una metodología que permita la identificación, recolección, preservación, análisis y presentación de evidencia digital generada por el usuario en el ordenador local que utilizó una aplicación web.
- Definir todos los artefactos y parámetros necesarios que serán utilizados durante la aplicación de la metodología.
- Evaluar esta propuesta, a través de pruebas de concepto y/o casos de estudio.

1.3. Tareas de Investigación

La metodología de investigación empleada es de carácter cuantitativo y se compone de 10 fases. A continuación, en la Figura 1.1, se describe el modelo de investigación seguida (Hernández Sampieri, Fernández Collado, y Baptista Lucio, 2014).

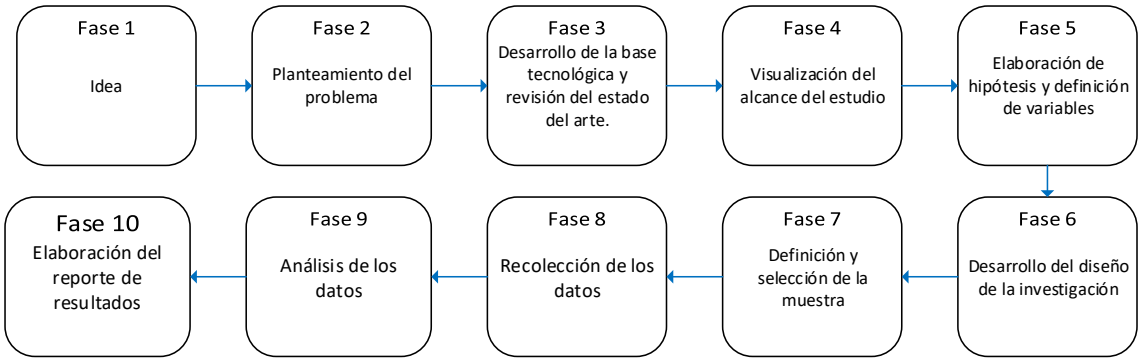


Figura 1.1: Modelo de investigación cuantitativo (Hernández Sampieri et al., 2014).

Cada fase se define de la siguiente manera:

1. **Idea:** El punto de partida es definido, el área de estudio a enfocarse se relaciona con la informática forense.
2. **Planteamiento del problema:** Se plantea un problema de estudio delimitado y concreto en el área. Se ha verificado la ausencia de una guía de buenas prácticas que permitan guiar una investigación forense enfocada en los artefactos web dejados en el ordenador en el lado del cliente, tomando en cuenta los lineamientos internacionales.

3. **Desarrollo de la base tecnológica y revisión del estado del arte:** Se considera todo lo que se ha estudiado anteriormente y se construye un marco teórico o base tecnológica. En este caso, se ha desarrollado una revisión de literatura siguiendo la metodología provista por Kitchenham (2004), sobre el manejo de la evidencia digital proveniente de entornos web en ordenadores del lado del cliente.
4. **Visualización del alcance del estudio:** Se ha delimitado la investigación planteando un objetivo general y cuatro objetivos específicos, junto con las preguntas de investigación que permiten abarcar toda la información requerida en el área de estudio Kitchenham (2004).
5. **Elaboración hipótesis:** Se genera la hipótesis previa a la recolección y análisis de los datos. En este caso particular se ha planteado una metodología que permita cubrir una investigación forense, en el ordenador del lado del cliente, desde el inicio hasta el cierre de esta; relacionada a la evidencia digital proveniente de entornos web.
6. **Desarrollo del diseño de la investigación:** Se planifica como se abordará la investigación y que métodos se utilizarán. Se ha diseñado realizar una prueba de conceptos para la evaluación de la metodología propuesta.
7. **Definición y selección de la muestra:** Se define un conjunto representativo para la realización de la investigación. Se ha asegurado que el escenario planteado para la evaluación de la metodología propuesta abarque gran parte del área de estudio y artefactos web que son dejados por aplicaciones en el sistema local.
8. **Recolección de los datos:** Se emplean procesos estandarizados y aceptados en la comunidad científica. Se ha conducido una investigación forense dentro del escenario de investigación planteado siguiendo la metodología propuesta.
9. **Análisis de los datos:** Los fenómenos encontrados deben ser analizados (se pueden emplear métodos estadísticos), señalando lo más relevante. Se dedica un apartado a tratar los resultados más relevantes de la realización de la investigación.
10. **Elaboración de reporte de resultados:** Se detalla lo más relevante de la investigación. Se incluye el reporte de resultados, junto con las conclusiones del trabajo que aseguran el cumplimiento de todos los objetivos planteados.

1.4. Estructura de Trabajo

Este trabajo está compuesto por 7 capítulos distribuidos de la siguiente manera:

El capítulo 1, introduce al lector en el contexto y alcance del trabajo, indica la metodología empleada y la organización del mismo.

El capítulo 2, contiene todos los conceptos necesarios para el desarrollo y entendimiento del presente trabajo de titulación.

El capítulo 3, presenta el estado actual, por medio de una revisión sistemática de literatura de las temáticas en las que se centra el trabajo que permitirá tener una vista objetiva de las soluciones existentes al problema planteado y determinará el estado de la investigación actual en la materia tratada en este trabajo de investigación.

El capítulo 4, presenta la contribución de este trabajo, contiene una metodología integral que brinda guías para identificar, recolectar, preservar, analizar y presentar un informe de la evidencia digital procedente de entornos web, en el ordenador del cliente, compuesta por una serie de actividades que permiten a dicha metodología ser aplicada en casos generales, que involucren evidencia digital proveniente, ya sea por el uso de navegadores o por el uso de aplicaciones de escritorio para interactuar con aplicaciones web.

El capítulo 5, contiene información detallada de una herramienta forense planteada y creada; con el objetivo de reducir los tiempos en la fase recolección de resultados.

El capítulo 6, contiene un escenario propuesto, en dónde se muestra la forma de aplicación de la metodología propuesta para su posterior evaluación junto con los resultados obtenidos al emplear la metodología, presentando un breve análisis de los resultados más relevantes en las fases de la misma.

El capítulo 7, contiene las conclusiones del trabajo y los trabajos futuros.

En la Figura 1.2, de autoría propia se muestra la estructura del trabajo a la vez que se cumplen las tareas de investigación realizadas.

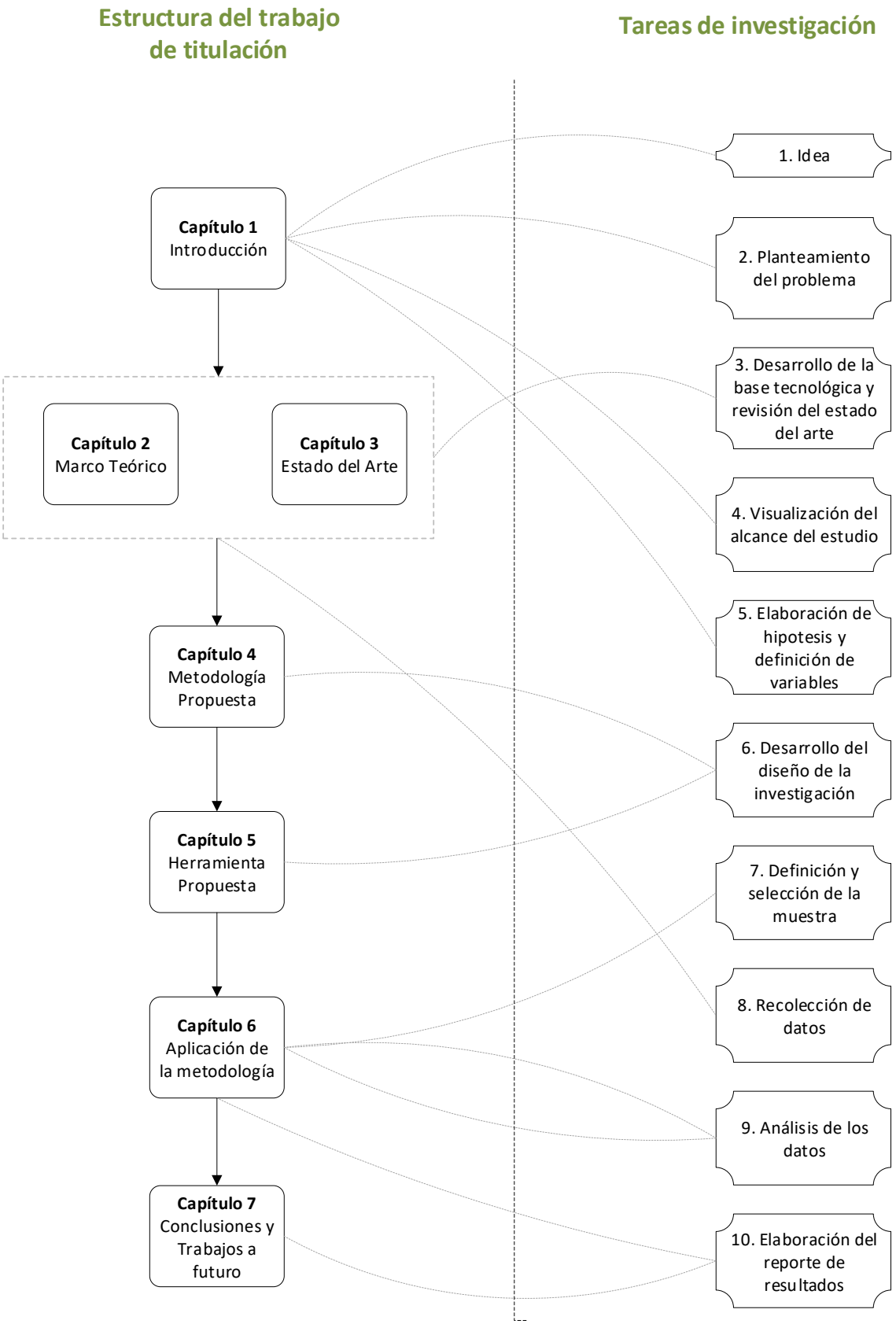


Figura 1.2: Estructura del trabajo de investigación.

Capítulo 2. Base Tecnológica

En este capítulo se dan a conocer los principales conceptos que representan la base y el sustento teórico del presente trabajo de titulación, los conceptos que forman parte de este ayudarán a esclarecer las dudas del lector y permitirán hacer que este trabajo sea autocontenido.

2.1 Informática forense. Conceptos y fundamentos.

Es importante que previo a definiciones más detalladas que servirán para el entendimiento del presente trabajo, se tenga claro que el área central del trabajo es la informática forense, la cual es una rama de las ciencias forenses (Guo, Jin, y Huang, 2010).

A continuación, se presentan las definiciones referentes a esta ciencia.

2.1.1 Ciencia Forense

A lo largo de historia varios sucesos han sido objeto de investigación, por lo que, para determinar cómo se produjo un hecho o determinar a los posibles responsables, surgieron las ciencias forenses. El término forense se deriva del latín “forensis” que significa “en audiencia pública o en público”, que a su vez proviene del latín “del foro” refiriéndose a una plaza pública utilizada para negocios judiciales u otros” (Guo et al., 2010). De manera que, el término “forense” puede ser comprendido como: el proceso de utilizar conocimiento técnico o científico para recolectar, analizar y presentar evidencia a las cortes (Guo et al., 2010). El término Ciencia Forense según Guo et al. (2010) es “la aplicación de técnicas científicas y principios para proveer pruebas a las investigaciones y resoluciones judiciales…”.

2.1.2 Informática Forense

Dado al incremento del uso de tecnologías computacionales en el día a día; cada vez son más frecuentes crímenes, delitos o contravenciones cometidos por medio de ordenadores (p. ej., estafas, posesión, carga de contenido ilegal), por ello surge la necesidad de una ciencia que estudie las diferentes tecnologías computacionales en busca de evidencia que pueda ser relevante para un suceso y su adecuado tratamiento; de ahí, la aparición de la informática forense (Casey, 2001).

Según Guo et al. (2010), la informática forense se originó a finales de la década de los 80, cuando los primeros profesionales de la aplicación de la ley lo utilizaron

para referirse al análisis de las computadoras independientes para obtener pruebas digitales. Además, añade que los informáticos emplean este término para técnicas aplicadas en redes, sistemas, periféricos, software, datos y/o usuarios para identificar actores, acciones o estados de interés.

Por otra parte, de acuerdo con Guo et al., (2010), Steve Hailey del Instituto de Cyber Seguridad, la Informática Forense está conceptualizada como: “La preservación, identificación, extracción, interpretación y documentación de la evidencia de una computadora, para incluir reglas de evidencia, procesos legales, integridad de la evidencia, reporte de la información encontrada y proveer una opinión técnica en una corte…”.

2.1.3 Evidencia Digital

En informática forense, la evidencia digital es uno de los términos más destacados. El término evidencia digital de acuerdo con la ISO/IEC 27037 (2012), se conoce como “información o datos, almacenados o transmitidos de forma binaria que pueden ser tomados en cuenta como evidencia o prueba.”.

Adicionalmente, Casey (2011), define la evidencia digital como “…cualquier dato almacenado o transmitido empleando un ordenador, que pueden apoyar o refutar una teoría…”.

2.1.4 Principio de intercambio de Locard

El punto de partida en el cual se basa gran parte de las ciencias forenses es el principio de Locard; el cual afirma que en cualquier escena del crimen o de suceso, el responsable de cualquier acto puede dejar parte de su material y llevarse algo (Helfgott, 2008).

2.1.5 Herramientas de análisis forense

Una vez identificados los artefactos (posible evidencia), es necesario una correcta recolección y análisis de los mismos, para facilitar estas acciones, tomando en cuenta que los ordenadores generan grandes cantidades de información, existen varias herramientas que permiten automatizar ciertos procesos de identificación, recolección y análisis de los artefactos dejados en el ordenador (Mahaju y Atkison, 2017; Sivaprasad y Jangale, 2012).

2.1.6 Evidencia Local Web

De acuerdo con varios autores, (Domingues y Frade, 2016; Morioka y Sharbaf, 2016; Ohana y Shashidhar, 2013), existen artefactos comunes, que pueden ser

encontrados en los sistemas operativos locales provenientes de la interacción con aplicaciones web. Estos artefactos o posibles evidencias pueden ser: archivos temporales, caché web, cookies, historiales de navegación. Los cuales se definen en la siguiente subsección dentro del ámbito web.

2.2 Web

La web, según Anderson (2016), es un conjunto de servicios fuertemente asociados, pudiendo encontrar diferentes términos para referirnos a estos servicios ya sean: blogs, wikis, podcasts, Really Simple Syndication (RSS) feeds, etc.; que facilitan la conectividad en la web en donde todos pueden agregar o editar información.

2.2.1 Arquitectura Cliente Servidor

Para que los usuarios puedan hacer uso de los servicios que se proveen en la web, la arquitectura más empleada es la llamada cliente-servidor. Esta arquitectura de acuerdo con Subhash (2009), en su libro titulado “Introduction to Client Server Computing”, manifiesta que se basa en una distribución de funciones entre dos procesos independientes y autónomos: cliente y servidor. En donde un cliente representa cualquier proceso que solicita algún servicio a los procesos del servidor. Mientras que el servidor es el proceso que provee los servicios solicitados por el cliente a través de una red (como Internet) (Subhash, 2009). En la Figura 2.1, se puede apreciar una representación básica de la arquitectura. El énfasis de este trabajo es el análisis forense en los ordeandores de lado del cliente.

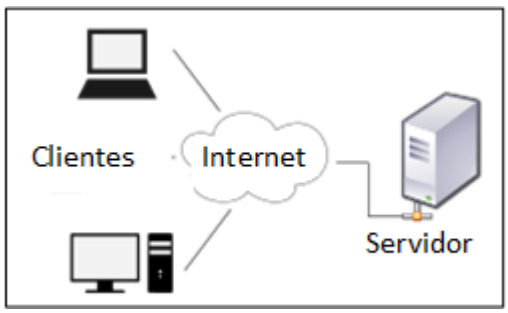


Figura 2.1: Representación arquitectura Cliente Servidor.

2.2.2 Aplicación web

Una aplicación web es uno de los medios más utilizados para acceder a recursos en Internet, éste es un programa o software que, según (Hausenblas, 2011), debe cumplir los siguientes requerimientos:

- Estar basado en el protocolo HTTP y URI.
- Para agentes usuarios, el formato de presentación es HTML.
- Para agentes de software, la interface primaria podría ser REST o basada en servicios web (como SOAP y UDDI).
- La aplicación opera sobre Internet.
- El número de usuarios simultáneos es indeterminado.

Las aplicaciones web que instalan los clientes en su ordenador (ej., Dropbox Desktop) para interactuar con las aplicaciones web, tienden a mantener información en el sistema operativo donde se hospedan, ya sean logs o archivos temporales que permitan obtener pistas de las actividades realizadas y de quien las realizó (Marturana, Me, y Tacconi, 2012; Morioka y Sharbaf, 2016).

2.2.3 Navegadores Web

De acuerdo al glosario de NIST Computer Security Center, un navegador web es un cliente de software empleado para visualizar contenido web («NIST», 2017). Pero algo más interesante, es que mientras se emplea este tipo de software, se almacena información importante en el sistema de archivos del ordenador donde se está ejecutando; por ejemplo, al abrir un sitio web por primera vez la caché del navegador almacena la página y elementos asociados (por ejemplo imágenes), cuando se interactúa posteriormente con el mismo sitio web, esta memoria caché es accedida y se localiza a los archivos correspondientes al sitio para cargarlos de manera más eficiente que la primera vez (por petición al servidor). Además con cada actividad que se realice, los archivos serán modificados y ubicados en el ordenador, pudiendo dejar pistas de quien está realizando las acciones (Casey, 2011; Morioka y Sharbaf, 2016). Para mejorar los servicios ofrecidos, además de la mencionada memoria caché, los navegadores suelen utilizar mecanismos que pueden generar potencial evidencia digital almacenada al lado del cliente.

A. Caché Web

Al interactuar con aplicaciones dentro de entornos web, se realizan varias solicitudes de información por parte del cliente al servidor, para solucionar de alguna forma el problema de tener un número excesivo de peticiones, existe la memoria caché web. Es así como Castellano y Fanelli (2009), en su libro “Web Personalization in Intelligent Environments”, establece que la caché web es “…un mecanismo desarrollado para reducir la latencia y el tráfico web.” El mecanismo consiste en almacenar parte de las páginas web solicitadas por cierto periodo de tiempo (Castellano y Fanelli, 2009).

B. Cookies

Otro mecanismo empleado por los navegadores para reducir la latencia son las cookies. Las cookies en la web son pequeños archivos de texto creados por un sitio web y enviados al disco duro del ordenador del cliente (Tipton, 2014). Las cookies almacenan nuestras elecciones cada vez que se navega a través de Internet, para de manera posterior cuando una URL (Uniform Resource Locator) es escrita, el navegador web contacta el servidor y solicita el sitio web específico para ser desplegado en el monitor, pero además el navegador busca en el disco duro si existe alguna cookie procedente de este sitio; de ser el caso el navegador traslada la información en el archivo de vuelta al sitio (Tipton, 2014).

C. Archivos Temporales

Por lo general, además de las cookies o la caché web, los navegadores requieren en algunos casos mayor cantidad de información para cargar un sitio web; es ahí en donde los archivos temporales son necesarios. Un archivo temporal de Internet, de acuerdo a Koreneff y Sims-McLean (2005), es un archivo que se encuentra en el disco duro del usuario, en donde un navegador almacena información (como texto, imágenes, números) de un sitio web (Koreneff y Sims-McLean, 2005).

Es importante acotar, que la mayoría de navegadores permiten eliminar estos archivos del sistema (Koreneff y Sims-McLean, 2005). Otra información bastante útil que proporcionan los navegadores corresponde a sus historiales, pues por lo general un navegador almacena de acuerdo con EC- Council (2009 distintos historiales:

- *Historiales de Navegación*: Provee información de los sitios web visitados, estableciendo su URL y fecha de acceso.
- *Historiales de Descargas*: Por lo general contiene metadatos de los archivos descargados de la web, como fecha, directorio de descarga y el dominio del cual el archivo fue descargado.
- *Cuentas y Contraseñas Guardadas*: Algunos navegadores, con el fin de mejorar el servicio a sus usuarios proveen la opción de almacenar sus datos de acceso a sitios web, los cuales pueden ser visibles posteriormente.

2.3 Computación en la nube

Un nuevo paradigma que está teniendo acogida es la computación en la nube, que ha cambiado la forma en la que se consumen los recursos de TI y es bien vista por los profesionales en el área por su capacidad de elasticidad en los recursos que ofertan (Galante y Bona, 2012). De acuerdo con el Instituto Nacional de Estándares y Tecnología (NIST) por sus siglas en inglés, la

computación en la nube es un modelo para posibilitar el acceso generalizado, conveniente y bajo demanda a través de la red a un conjunto de recursos (como redes, servidores, almacenamiento, aplicaciones o servicios) (Mell y Grance, 2011). A continuación, revisaremos sus diferentes modelos de servicio.

2.3.1 Modelos de Servicio

Para poder cumplir con su definición la computación en la nube ofrece tres modelos de servicios para su implementación (Mell y Grance, 2011). El presente trabajo de investigación está enfocado en el primer modelo (SaaS); desde la perspectiva del usuario o el lado del cliente como se puede apreciar en la Figura 2.3. Los modelos de servicio de la computación en la nube se describen a continuación:

A. ***Software como Servicios (SaaS):***

Provee la capacidad al consumidor de utilizar las aplicaciones del proveedor ejecutándose en una infraestructura en la nube. La aplicación puede ser accedida mediante una interfaz cliente.

B. ***Plataforma como Servicio (PaaS):***

Provee la capacidad al consumidor de desplegar, en una infraestructura en la nube, sus aplicaciones creadas o adquiridas por los mismos. Las librerías, servicios y herramientas son provistas por el proveedor; el consumidor solo tiene control sobre la aplicación desplegada y sus configuraciones.

C. ***Infraestructura como Servicio (IaaS):***

La capacidad provista al consumidor son provisiones de procesamiento, almacenamiento, redes y otros recursos computacionales fundamentales, donde el consumidor puede desplegar y ejecutar arbitrariamente software; estas pueden ser aplicaciones de software o sistemas operativos.

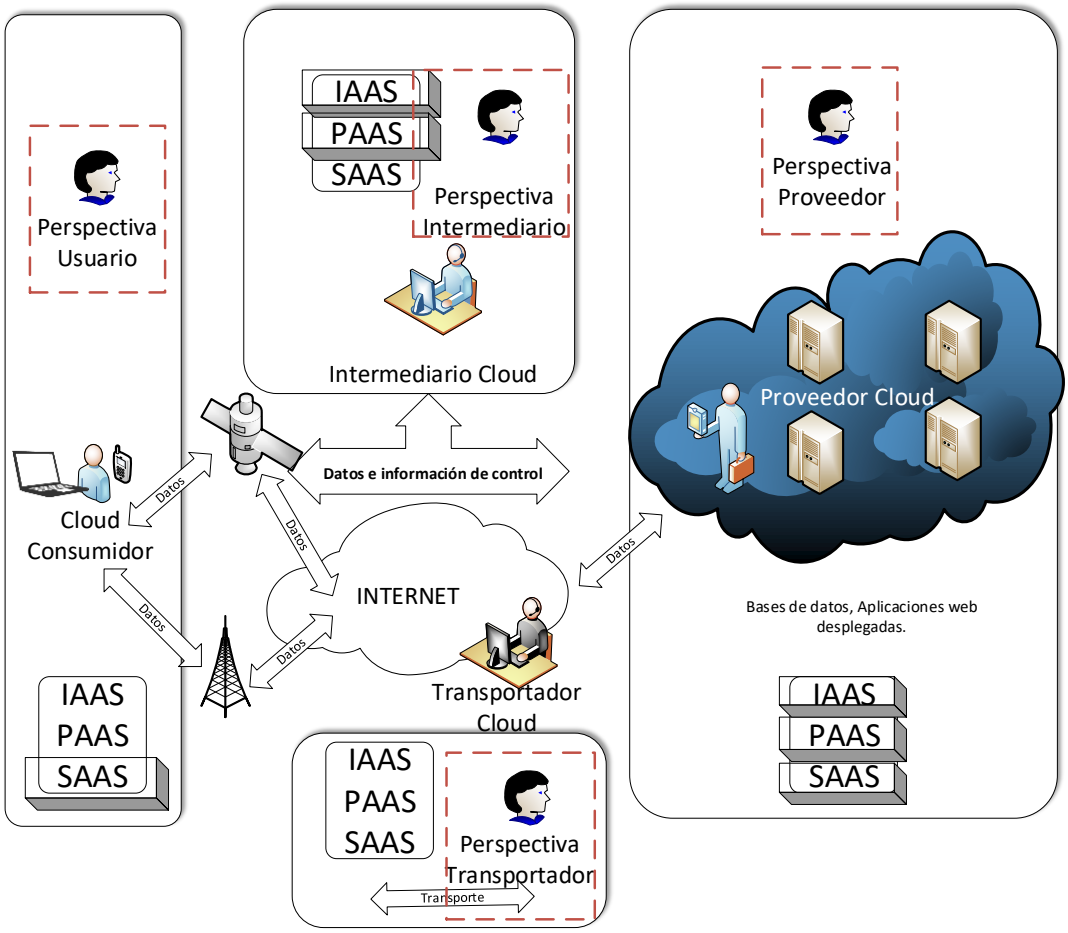


Figura 2.2: Perspectivas y modelos de computación en la nube (cloud) (Jara y Cedillo, 2017).

2.4 Estándares, normas y regulaciones

En el campo de la informática forense, existen normas internacionales y regulaciones en la ley que pueden servir en algunos casos de base; para realizar una investigación forense. A continuación, se presentan las regulaciones y los estándares internacionales más relevantes que aportan al presente trabajo de titulación.

2.4.1 Delito Informático

Para dar un breve preámbulo de las regulaciones en nuestro medio, es importante conocer que se considera delito informático. Según Reyes et al., (2011), considera un delito o crimen informático, a cualquier incidente donde una víctima se vea afectada, y el perpetrador del acto cometió el hecho con una computadora (Reyes, Brittson, O'Shea, y Steele, 2011). Dentro de las regulaciones locales, de acuerdo al Código Orgánico Integral Penal (COIP), los artículos referidos específicamente a los sistemas de información son los

artículos comprendidos entre 229 al 234 del COIP. Pese a esto, con la evolución de las tecnologías de la información, existen otros artículos que referencian posibles delitos informáticos, en la tabla 2.1 se enumeran los artículos más relevantes de la ley ecuatoriana para delitos informáticos:

Tabla 2.1: Artículos referidos a delitos informáticos de la ley ecuatoriana

Artículo	***Descripción***
178	Hace referencia a la violación de la intimidad, donde hace hincapié al acceso, reproducción, difusión de datos personales incluyendo los datos contenidos en dispositivos; que sean difundidos por cualquier medio.
190-194	Trata de la apropiación fraudulenta por medios electrónicos.
229-234	Trata de los delitos en contra de la seguridad de los activos de sistemas de información y comunicación.
500	Hace referencia a todo lo que se considera como contenido digital.

Revisadas las regulaciones más relevantes, para los posibles crímenes informáticos tipificados en el COIP, también surge la importancia de revisar que estándares pueden emplearse como guías para seguir un proceso de investigación.

2.4.2 ISO/IEC 27037: Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital.

Esta ISO proporciona guías para actividades específicas en el manejo de evidencia digital, dichas actividades hacen referencia a la identificación, recolección, preservación de evidencia digital potencial. Provee guías para:

- Medios de almacenamiento usados en computadores estándares.
- Dispositivos móviles.
- Sistemas móviles de navegación.
- Computadores estándares y conexiones de red.
- Redes basadas en los protocolos TCP/IP y otros.

2.4.3 ISO/IEC 27042: Directrices para el análisis e interpretación de la evidencia digital

Provee guías en el análisis y la interpretación de la evidencia digital, de forma que se logre garantizar o abordar cuestiones de continuidad, validez, reproductibilidad y repetitividad. Contiene, además, buenas prácticas para la selección, diseño e implementación de un proceso analítico y recoger suficiente información que permita que dichos procesos puedan ser sometidos a escrutinios independientes cuando sea necesario.

En resumen, este estándar provee un marco común, para lidiar con incidentes en sistemas de seguridad analizando e interpretando los elementos propios del incidente. El cual puede ser empleado para asistir a la implementación de nuevos métodos.

Capítulo 3. Estado del Arte

En este capítulo se muestran los estudios que se han realizado en el área de la informática forense referida a la evidencia digital procedente de sitios web; enfocados en el ordenador del lado del cliente, para tener una visión global de que como se está abordando el problema, a través de una revisión sistemática de literatura.

En la primera parte de este capítulo, sección 3.1, se detalla el método aplicado para recolectar la información relevante para la revisión sistemática.

En la sección 3.2 se presenta la ejecución de la revisión sistemática sobre el manejo de evidencia digital proveniente de aplicaciones web alojadas en el ordenador del cliente.

3.1 Introducción a una revisión sistemática

La revisión sistemática es una metodología utilizada para identificar, evaluar e interpretar toda la investigación relevante existente para una pregunta de investigación o temática en particular, ésta permite reportar toda la evidencia que compete a una temática (Kitchenham, 2004).

Para realizar una revisión sistemática se consideran estudios individuales llamados estudios primarios; al formar una revisión sistemática se obtiene una forma de estudio secundario. Este tipo de estudios se basa en un protocolo muy bien elaborado y una metodología que permite hacer de una revisión del estado del arte, un producto científico repetible y formal; los tres procesos principales son: planeación, conducción de la revisión y el reporte de la revisión (Kitchenham, 2004).

3.1.1 Estudios Relacionados

Existen algunos estudios secundarios relacionados al manejo de evidencia digital, proveniente de entornos web (Guo et al., 2010; Garfinkel, 2010; Simou et al., 2014; Hatole y Bawiskar, 2017; Kaur, Kaur, y Khurana, 2016; Bhosale, Mitkal, Pawar, y Paranjape, 2016). En el siguiente párrafo se presenta una breve descripción de los mismos.

Guo et al., (2010), presenta definiciones y principios referentes a informática forense de manera general. No se consideran especificaciones para obtener evidencia del lado del cliente en cuanto a evidencia proveniente de entornos web (como lugares de almacenamiento, tipo de información). Por otro lado, Garfinkel (2010), presenta una revisión de la literatura, la cual está dirigida a los problemas

de los procesos forenses actuales y retos en un futuro cercano; sin embargo, el autor no cubre el área de estudio de la evidencia proveniente de entornos web en el lado del cliente. Simou et al., presenta una revisión de informática forense en la nube (Cloud Forensics terminología en inglés); los autores se enfocan en soluciones y técnicas disponibles presentadas en estudios primarios que tienen aplicabilidad en la computación en la nube (principalmente en el modelo de servicio SaaS). Además, provee guías generales a ser consideradas respecto a los artefactos que puedan ser encontrados en dicho modelo de servicio. Sin embargo, el estudio no presenta detalles acerca del manejo de la evidencia digital proveniente de entornos web del lado del cliente. Hatole y Bawiskar (2017), proponen una revisión de literatura de análisis forense en el área de correos electrónicos, el cual está enfocado en herramientas disponibles para el manejo de datos de los mismos. Sin embargo, no cubren áreas para casos generales y artefactos de otros sitios o servicios web. Kaur et al. (2016), por su parte, propone una revisión de literatura de ciber forense, el autor presenta detalles generales y sintetiza información acerca de herramientas para el manejo de evidencia digital; sin embargo, no se abordan temas específicos sobre la evidencia de entornos web del lado del cliente: lugares, dependencias de plataforma de las herramientas. Por su lado, Bhosale et al. (2016), propone una revisión de informática forense donde se definen guías para recolectar evidencia digital de ambientes web sin ser éste el enfoque central, por lo cual no cubren el lado del cliente.

Consecuentemente, a pesar de que existen varios estudios secundarios presentados estos presentan dos limitaciones principales:

I. La mayoría de los estudios no mencionan los estándares internacionales en sus investigaciones, o como estos están participando en ellas.
II. La mayoría de estos no se enfocan en aspectos relacionados con la informática forense del lado del cliente.

3.2 Revisión sistemática sobre el manejo de evidencia digital web

Con el objetivo de realizar un estado del arte preciso, se ha realizado una investigación acerca de los aspectos más relevantes en el ámbito de la gestión de evidencia digital proveniente de aplicaciones desplegadas en entornos web, en el ordenador del cliente. Para ello se ha empleado un método que permite identificar toda la información existente, dicho método permite obtener una revisión sistemática, considerando las recomendaciones provistas en los trabajos de B. Kitchenham (2004), (2009).

Para la presente revisión sistemática, se han considerado las tres fases recomendadas: planeación, conducción y reporte de resultados.

3.2.1 Fase de Planificación

En la fase de planificación se consideraron 6 pasos:

- **A.** Establecer la pregunta de investigación y sub-preguntas que nos permitan abarcar todo nuestro campo de estudio.
- **B.** Definición de la estrategia de búsqueda
- **C.** Selección de los estudios primarios
- **D.** Evaluación de la calidad
- **E.** Definición de la estrategia de extracción
- **F.** Selección de métodos de síntesis

A. Pregunta de investigación

El objetivo de esta revisión sistemática es examinar cuáles son los aspectos considerados para la gestión de evidencia digital proveniente de entornos web del lado del cliente, desde el punto de vista de la siguiente pregunta de investigación:

"¿Qué procedimientos forenses son considerados por los investigadores forenses para el manejo de evidencia digital situada en el lado del cliente proveniente de entornos web?"

Esta pregunta de investigación nos permitirá resumir el conocimiento actual sobre las recomendaciones existentes para el manejo de evidencia web desde la perspectiva del cliente e identificar algunas áreas de investigación futuras.

Para dar soporte a esta pregunta de investigación, se han planteado las siguientes sub-preguntas.

RQ1: ¿Qué tipo de evidencia web se puede encontrar en la computadora del cliente?

RQ2: ¿En qué lugar de la computadora del cliente se puede encontrar evidencia digital de entornos web?

RQ3: ¿Qué herramientas se pueden utilizar para automatizar el manejo de evidencia web?

RQ4: ¿Cómo preservar la evidencia digital para garantizar su integridad?

RQ5: ¿Cómo los estándares están siendo empleados en el manejo de la evidencia digital?

B. Definición de las estrategias de búsqueda

Primero, se ha definido una fecha acorde a un hito como punto de partida para seleccionar los estudios primarios; en este estudio, se ha definido el surgimiento de la web 2.0 en el año 2004, por lo que se han considerado únicamente estudios posteriores a este año. Para desarrollar esta investigación se han elegido diferentes recursos, realizando búsquedas automatizadas como manuales. Con respecto a las búsquedas manuales, se ha buscado en las ediciones de las siguientes conferencias, revistas y libros:

- International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).
- IEEE Security and Privacy Workshops (HST).
- International Conference on Utility and Cloud Computing (UCC).
- International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE).
- Workshop de Investigadores en Ciencias de la Computación (WICC).
- International Conference on Cybercrime Forensics Education and Training (CFET).
- Computer IEEE
- IEEE Cloud Computing
- International Journal of Electronic Security and Digital Forensics
- IEEE Transactions on Information Forensics and Security
- ACM Transactions on Information and System Security

Con respecto a las búsquedas automatizadas; las bibliotecas digitales usadas son ACM, IEEE Xplore, Springer Link y Science Direct. Adicionalmente, la cadena de búsqueda empleada para la búsqueda es la siguiente: "((FORENSIC) AND (WEB OR BROWSER OR CLOUD) AND (DIGITAL) AND (EVIDENCE))". Cabe recalcar que se experimentó con varias cadenas de búsqueda obteniendo los mejores resultados con la cadena presentada, también se limitó el año de desde la fecha hito (2005) hasta la actualidad.

C. Selección de estudios primarios

Cada estudio procedente de las búsquedas automatizadas y manuales ha sido evaluado para decidir si es incluido o excluido, inicialmente considerando su título, resumen y palabras clave.

Los criterios de inclusión son:

- Estudios que presenten métodos para identificar, recolectar, preservar, analizar o presentar evidencia digital provenientes de sitios web.
- Estudios que presenten herramientas que permitan automatizar el proceso de informática forense.

- Estudios que presenten métodos que nos permitan salvaguardar la evidencia digital.

Por otro lado, se han excluido los estudios que contengan los siguientes criterios:

- Estudios introductorios para problemas específicos, libros y workshops.
- Estudios duplicados en diferentes repositorios de información.
- Estudios cortos de menos de cinco páginas.
- Estudios que no hayan sido escritos en inglés.

Además, la estrategia para obtener los datos ha sido definida de tal forma que permita responder las preguntas de investigación.

D. Evaluación de la Calidad

De manera adicional a los criterios de inclusión/exclusión, se ha considerado como un punto crítico la evaluación de la calidad de los estudios seleccionados. Para ello nos hemos planteado un cuestionario con las siguientes preguntas:

- ¿El estudio presenta cuestiones relacionadas con los procedimientos de evidencia digital proveniente de aplicaciones web en la computadora local?
- El estudio presenta soluciones a los problemas de tratar evidencia digital proveniente de ambientes web en la computadora local.
- ¿El estudio ha sido publicado en una revista o conferencia relevante?
- ¿El estudio ha sido citado por otros autores?

El puntaje para cada pregunta cerrada será la media aritmética de todos los puntajes individuales de los revisores. La suma de los puntajes de las 4 preguntas cerradas de cada estudio provee un puntaje que ha sido empleado para excluir estudios de la revisión sistemática, además este valor puede ser empleado para identificar estudios representativos.

E. Definición de las Estrategias de Extracción

La estrategia de extracción empelada está basada en cada una de las posibles respuestas de las sub-preguntas que fueron definidas. En la Tabla 3.1 se muestran los diferentes criterios que responden a las diferentes preguntas de investigación.

Tabla 3.1: Preguntas de Investigación y sus respectivos criterios

RQ1: ¿Qué tipo de evidencia digital se puede encontrar en la máquina del cliente?		
EC1	Tipo de Artefactos	Indicadores de navegación

		Archivos temporales (cachés, cookies, otros)
RQ2: ¿En qué lugares del ordenador local se puede encontrar evidencia web?		
EC2	Perspectiva	Cliente
		Tránsito
		Servidor
EC3	Orígenes Locales	Navegador
		Aplicaciones de Escritorio
		Logs del Sistema
RQ3: ¿Qué herramientas se puede emplear para automatizar procesos de manejo de evidencia digital web?		
EC4	Tipo de Sesión	General
		Sesión Privada/incógnita
		Sesión Portable
EC5	Dependencias	Plataforma
		Navegador
RQ4: ¿Cómo preservar la evidencia recolectada para garantizar su integridad?		
EC6	Preservación de la evidencia digital	Métodos de Autenticación
		Métodos de Integridad
RQ5: ¿De qué manera los estándares son empleados en el manejo de la evidencia digital?		
EC7	Estándares relacionados en las soluciones	ISO/IEC 27037
		ISO/IEC 27042
		ISO/IEC 27041
		ISO/IEC 27050
		ISO/IEC 27017

De acuerdo a la Tabla 3.1, los estudios seleccionados referidos a EC1 pueden ser clasificados en uno o más tipo de artefactos existentes en la computadora del cliente (ej., indicadores de navegación en logs de eventos del sistema, cachés, cookies y otros archivos temporales). Los estudios seleccionados bajo los criterios de tipo de artefactos se aprecian en la Tabla 3.2

Tabla 3.2: Estudios seleccionados respecto al tipo de artefacto.

Indicadores de navegación	(Baca, Cosic, y Cosic, 2013; Chow et al., 2005; Gupta y Mehtre, 2013; Jang y Kwak, 2015; Levinson, Stackpole, y Johnson, 2011; Majeed, Zia, Imran, y Saleem, 2015; Marturana et al., 2012; Matsumoto y Sakurai, 2014; Mehreen y Aslam, 2015; Mirza, 2008;

	Morioka y Sharbaf, 2016; Nair y Ajeena, 2014; Nalawade, Bharne, y Mane, 2016; Oh et al., 2011; Ohana y Shashidhar, 2013; Said, Mutawa, Awadhi, y Guimaraes, 2011; Sivaprasad y Jangale, 2012)
Archivos Temporales (ej., cachés, cookies, otros)	(Baca et al., 2013; Castiglione, Cattaneo, y Santis, 2011; Chen et al., 2015; Farina, Scanlon, Le-Khac, y Kechadi, 2015; Gupta y Mehtre, 2013; Jang y Kwak, 2015; Mahaju y Atkison, 2017; Majeed et al., 2015; Marturana et al., 2012; Matsumoto y Sakurai, 2014; Mehreen y Aslam, 2015; Morioka y Sharbaf, 2016; Nalawade et al., 2016; Oh et al., 2011; Ohana y Shashidhar, 2013; Said et al., 2011; Simou et al., 2014; Sivaprasad y Jangale, 2012).

En el criterio EC2, un estudio puede ser clasificado en una o más perspectivas, dependiendo de donde se encuentra la información almacenada o situada (Morioka y Sharbaf, 2016): (i) Información almacenada en el servidor (proveedor Cloud, servidor web); (ii) Información en tránsito (entre el cliente y el servidor) (iii) Información el lado del cliente: si la información se encuentra en la computadora del cliente, consecuentemente la investigación es llevada a cabo ahí. La Tabla 3.3 muestra los estudios seleccionados de acuerdo a las diferentes perspectivas

Tabla 3.3: Estudios seleccionados respecto a las perspectivas de investigación.

Cliente	(Choo et al., 2017; Farina et al., 2015; Howden, Liu, Ding, Zhan, y Lam, 2013; Jang y Kwak, 2015; Lee et al., 2005; Matsumoto y Sakurai, 2014; Morioka y Sharbaf, 2016; Nair y Ajeena, 2014; Raju y Geethakumari, 2016; Roussev y McCulley, 2016; Simou et al., 2014)
Tránsito	(Chen et al., 2015; Choo et al., 2017; Farina et al., 2015; Jang y Kwak, 2015; Miranda Lopez, Moon, y Park, 2016; Morioka y Sharbaf, 2016; Nair y Ajeena, 2014)
Servidor	(Chen et al., 2015; Choo et al., 2017; Farina et al., 2015; Howden et al., 2013; Jang y Kwak, 2015; Lee et al., 2005; Matsumoto y Sakurai, 2014; Miranda Lopez et al., 2016; Simou et al., 2014)

En cuanto al criterio EC3, un estudio analizado puede ser clasificado en cuanto a los medios que generan evidencia en la computadora en el lado del cliente (ej., navegadores, aplicaciones de escritorio, logs) (Oh et al., 2011), (Marturana et al., 2012). Los estudios seleccionados para cubrir este criterio se muestran en la Tabla 3.4.

Tabla 3.4: Estudios seleccionados respecto a las perspectivas de investigación.

Navegador web	(Baca et al., 2013; Castiglione et al., 2011; Chow et al., 2005; Farina et al., 2015; Gupta y Mehtre, 2013; Howden et al., 2013; Jang y Kwak, 2015; Lee et al., 2005; Mahaju y Atkison, 2017; Majeed et al., 2015; Marturana et al., 2012; Matsumoto y Sakurai, 2014; Mehreen y Aslam, 2015; Mirza, 2008; Nair y Ajeena, 2014; Nalawade et al., 2016; Oh et al., 2011; Ohana y Shashidhar, 2013; Said et al., 2011; Sivaprasad y Jangale, 2012)
Aplicaciones de escritorio	(Chow et al., 2005; Farina et al., 2015; Gupta y Mehtre, 2013; Majeed et al., 2015; Marturana et al., 2012; Matsumoto y Sakurai, 2014; Mehreen y Aslam, 2015; Miranda Lopez et al., 2016; Mirza, 2008; Morioka y Sharbaf, 2016; Oh et al., 2011; Roussev y McCulley, 2016; Simou et al., 2014; Sivaprasad y Jangale, 2012)
Registros del sistema	(Farina et al., 2015; Garfinkel, 2010; Gupta y Mehtre, 2013; Mehreen y Aslam, 2015; Mirza, 2008; Morioka y Sharbaf, 2016; Ohana y Shashidhar, 2013; Said et al., 2011; Sivaprasad y Jangale, 2012)

Continuando con el criterio EC4, un estudio puede ser clasificado respecto al tipo de sesión en la que se da la interacción (ej., privada, portable, normal) con se aprecia en estudios (Ohana y Shashidhar, 2013; Said et al., 2011). En la Tabla 3.5, Se aprecian los estudios seleccionados de acuerdo al tipo de sesión.

Tabla 3.5: Estudios seleccionados respecto al tipo de sesión abarcado.

General	(Baca et al., 2013; Castiglione et al., 2011; Chow et al., 2005; Farina et al., 2015; Gupta y Mehtre, 2013; Jang y Kwak, 2015; Mahaju y Atkison, 2017; Majeed et al., 2015; Marturana et al., 2012; Matsumoto y Sakurai, 2014; Mehreen y Aslam, 2015; Mirza, 2008; Nair y Ajeena, 2014; Nalawade et al., 2016; Oh et al., 2011; Said et al., 2011; Sivaprasad y Jangale, 2012)
Sesión Privada/ incógnita	(Gupta y Mehtre, 2013; Nair y Ajeena, 2014; Nalawade et al., 2016; Ohana y Shashidhar, 2013; Said et al., 2011)
Sesión Portable	(Gupta y Mehtre, 2013; Nair y Ajeena, 2014; Ohana y Shashidhar, 2013)

Por su parte el criterio EC5, permite clasificar un estudio respecto a las dependencias que las soluciones planteadas puedan tener, es así que si utilizamos ciertas herramientas para una investigación estas pueden ser dependientes ya sea de plataforma (sistema operativo) o dependientes del navegador (Firefox, Opera, Google Chrome, etc.). En la Tabla 3.6, se muestran los estudios seleccionados de las dependencias seleccionadas.

Tabla 3.6: Estudios seleccionados acorde a las dependencias planteadas.

Plataforma	(Majeed et al., 2015; Marturana et al., 2012; Mehreen y Aslam, 2015; Mirza, 2008; Ohana y Shashidhar, 2013)
Navegador	(Mahaju y Atkison, 2017; Marturana et al., 2012; Oh et al., 2011; Ohana y Shashidhar, 2013)

En cuanto al criterio EC6, un estudio puede ser clasificado en uno o más métodos para preservar la evidencia digital: métodos de autenticación, los cuales protegen a la evidencia de accesos no autorizados, y mantienen registrado cada acceso de personal autorizado; para estos propósitos existen varios métodos empleados por expertos (Wang, 2010); métodos de integridad, los cuales resaltan la importancia de mantener la evidencia digital sin variaciones o corrupciones, por lo que de la misma manera existen métodos para asegurar la integridad de la evidencia (Lee et al., 2005). La Tabla 3.7, muestra los estudios seleccionados respecto a la preservación de la evidencia digital.

Tabla 3.7: Estudios seleccionados respecto a la preservación de la evidencia digital.

Métodos de Autenticación	(Farina et al., 2015; Garfinkel, 2010; Gupta y Mehtre, 2013; Howden et al., 2013; Lee et al., 2005; Morioka y Sharbaf, 2016; Saleem, Popov, y Dahman, 2011)
Métodos de Integridad	(Baca et al., 2013; Chen et al., 2015; Chow et al., 2005; Farina et al., 2015; Jang y Kwak, 2015; Lee et al., 2005; Majeed et al., 2015; Morioka y Sharbaf, 2016; Nair y Ajeena, 2014; Ohana y Shashidhar, 2013; Roussev y McCulley, 2016; Said et al., 2011; Saleem et al., 2011; Wang, 2010)

Finalmente, con respecto al criterio EC7, un estudio puede ser clasificado en uno o más estándares que son empleados en la investigación de informática forense; los estándares que se adaptan mejor al análisis forense en ambientes web es la familia de la ISO/IEC 27000 especialmente la 27017, 27037, 27041, 27042 y el 27050, porque proveen guías para la correcta gestión de la evidencia digital y lineamientos de seguridad. Los estudios que han sido seleccionados, respecto a los estándares planteados, se muestran en la Tabla 3.8.

Tabla 3.8: Estudios de los estándares de la familia 27000 seleccionados.

ISO/IEC 27037	(Council, 2013; Hibbard, 2014; Howden et al., 2013; Lee et al., 2005; Miranda Lopez et al., 2016; Jaromír Veber y Klima, 2015; Jaromír Veber y Klíma, 2014; Jaromir Veber y Smutny, s. f.; Wang, 2010)

ISO/IEC 27042	(Council, 2013; Miranda Lopez et al., 2016; Jaromír Veber y Klima, 2015; Jaromír Veber y Klíma, 2014)
ISO/IEC 27041	(Hibbard, 2014; Jaromír Veber y Klima, 2015)
ISO/IEC 27050	(Hibbard, 2014; Jaromír Veber y Klima, 2015)
ISO/IEC 27017	(Council, 2013; Jaromír Veber y Klima, 2015)

F. Métodos de Síntesis

Se han aplicado tanto métodos cuantitativos como cualitativos. La síntesis de cuantitativa está basada en:

- Contabilizando los estudios primarios que han sido clasificados en cada respuesta de nuestras sub-preguntas de la investigación.
- Contabilizando el número de estudios encontrados en cada una de las fuentes bibliográficas.

Las síntesis cualitativas están basadas en incluir varios estudios representativos para cada sub pregunta considerando los resultados de la evaluación de calidad.

3.2.2 Fase de Conducción

Acorde a la metodología para la revisión sistemática los resultados fueron seleccionados de acuerdo a los criterios de inclusión.

En esta fase se encontró algunos estudios que fueron publicados en más de una revista o conferencia, en estos casos se ha seleccionado la versión más completa del estudio. Así mismo en publicaciones iguales consideramos el orden de búsqueda: IEEEXplore, ACM, Springer Link y Science Direct.

Un total de 37 publicaciones de 1415 documentos fueron seleccionadas de acuerdo a los criterios de inclusión/excusión indicados en la subsección anterior, Los estudios encontrados en las bibliotecas digitales están distribuidos de la siguiente manera: 11% en ACM, 74% en IEEE Xplore, 8% en Science Direct y 7% en Springer Link como se aprecia en la Figura 3.1. En la extracción de los trabajos finales se contemplaron los siguientes hechos:

- Algunos estudios fueron publicados en más de una revista o conferencia. Se procedió a seleccionar la versión más completa.
- Algunos estudios se encontraron en más de una fuente. En este caso se consideró el estudio una sola vez de acuerdo al orden de fuentes planteado.

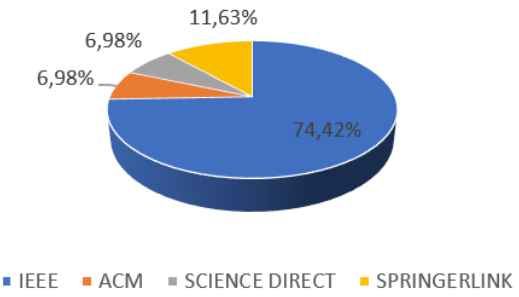


Figura 3.1: Porcentaje de estudios aceptados clasificados por las bibliotecas digitales.

3.2.3 Reporte de Resultados

En esta sección se reporta los resultados encontrados para las preguntas de investigación planteadas para la realización de esta revisión sistemática. Los artículos seleccionados responden las preguntas de investigación. Es así, que se presenta un reporte con los resultados más relevantes de la investigación. Para realizar el reporte se ha organizado el mismo en los pasos esenciales que involucra una investigación forense de acuerdo con la ISO/IEC 27037(2012) y su complemento las ISO/IEC 27042 (2015): i) identificación, ii) recolección, iii) preservación, iv) análisis y reporte de la evidencia digital y finalmente se ha considerado v) una pequeña revisión acerca de cómo los estándares están siendo empleados en estudios de expertos.

i. Identificación de la evidencia digital web

Como primer paso de una investigación forense, se ha considerado la fase de identificación. Esta fase en primer lugar depende de las diferentes perspectivas web (proveedor servidor/cloud, transporte/red, cliente/usuario). En la Figura 2.1 y 2.2 se pueden apreciar las diferentes perspectivas en la arquitectura cliente-servidor y las perspectivas computación en la nube respectivamente, donde una investigación forense puede ser realizada.

Cuando la evidencia está en el servidor lo recomendable es adquirir la información directamente del proveedor pese a los problemas que implican las diferentes jurisdicciones, por otro lado, si el objeto de la investigación se encuentra en un ambiente en la nube (cloud) en ciertos casos es posible utilizar el monitor de máquinas virtuales para recabar información (Morioka y Sharbaf, 2016). Otra forma de obtener información cuando la misma se encuentra en el servidor es mediante el uso de APIs provistas por los fabricantes de aplicaciones alojadas en entornos web, esto para permitir a investigadores extraer información (Howden et al., 2013). Siguiendo la misma recomendación también es posible analizar los datos que persisten en aplicaciones web o SaaS mediante APIs y estructuras de datos para extraer registros de aplicaciones SaaS (por

ejemplo, Google Docs, Slides, Sheets) (Matsumoto y Sakurai, 2014; Roussev y McCulley, 2016), otra opción cuando la información está en el servidor; es intentar acceder a la cuenta del usuario (Jang y Kwak, 2015).

Cuando la evidencia se encuentra en la perspectiva de tránsito Jang y Kwak (2015), recomiendan capturar la información volátil porque esta no puede ser modificada (Jang y Kwak, 2015); mientras que otra alternativa, es buscar información de las actividades o interacción del usuario con aplicaciones web en el nodo proveedor de servicio de Internet; sin embargo esta actividad es complicada debido a que las leyes y regulaciones de cada país son diferentes y pueden presentar restricciones para garantizar la privacidad de los usuarios. En este caso es necesario que la autoridad legal emita una orden que de acceso al investigador a la información requerida (Morioka y Sharbaf, 2016).

Finalmente, en la perspectiva del cliente (área de este trabajo de investigación); es decir cuando la evidencia se encuentra en el ordenador del cliente (perspectiva de cliente o usuario), Morioka y Sharbaf (2016); sugiere que es necesario buscar archivos locales que son dejados por las aplicaciones y navegadores en las máquinas locales, de la misma manera cuando el usuario interactúa en con aplicaciones SaaS en la nube algunos fragmentos de archivos y caché son dejados en el ordenador local (Farina et al., 2015; Morioka y Sharbaf, 2016). Otros autores proponen un análisis avanzado de evidencia web de los navegadores basados en el análisis de historiales, cookies, cachés, páginas favoritas. Además presentan guías para la recuperación de información eliminada debido a que varios navegadores permiten a los usuarios eliminar sus registros (Chen et al., 2015; Gupta y Mehtre, 2013; Oh et al., 2011); sin embargo, estos estudios no presentan una guía íntegra sobre como preservar la evidencia recolectada.

Adicionalmente, Jang y Kwak (2015) proponen una metodología para identificar, recolectar y analizar evidencia web pero este trabajo está enfocado en un aspecto puntual que es únicamente el análisis de redes sociales; logrando identificar conversaciones de chats y perfiles de usuario (Jang y Kwak, 2015).

Por otra parte, identificando la procedencia de la evidencia, la evidencia web puede provenir del uso de aplicaciones de escritorio que se utilizan para interactuar con las aplicaciones web; puesto que las aplicaciones almacenan información en el sistema local, se puede encontrar evidencia web como logs de sincronización, archivos recientemente modificados, eliminados para el caso de aplicaciones como Dropbox (Marturana et al., 2012; Mehreen y Aslam, 2015). En otro estudio, basado también en el campo específico de redes sociales se pueden encontrar interesantes evidencias de la interacción del usuario con estas aplicaciones, por ejemplo de Facebook se pudo recolectar imágenes, estados, URLs (Baca et al., 2013).

Por otro lado, en otros estudios (Ohana y Shashidhar, 2013; Sivaprasad y Jangale, 2012), se presentan guías y recomendaciones para recolectar información procedente de navegadores web, donde se ha recuperado evidencia web procedente del caché de navegación, archivos temporales del disco duro, cookies. Examinando estos artefactos, se pudo encontrar información acerca de: cuentas de correo, imágenes, videos e historial. Otros procesos para localizar evidencia web está basada en el navegador Firefox y se ha podido encontrar evidencia web relevante procedente de dicho navegador como: sitios web visitados, cookies, descargas, favoritos e ingresos de sesión (Mahaju y Atkison, 2017). También Nalawade et al., (2016), en su trabajo recolecta evidencia web como memorias cachés, historiales, cookies de diferentes navegadores. Por otro lado, Castiglione et al., (2011) se enfoca en las imágenes (fotografías) obtenidas de redes sociales, estas imágenes tienen diferentes tamaños dependiendo de la red social que se origina, la información que la imagen contiene como el titulo puede ayudar a identificar la procedencia de la misma. Además es posible obtener evidencia web incluso cuando se utilizan sesiones privadas, esto puede ser por que el navegador utiliza extensiones que no consideran la privacidad de la sesión (Nalawade et al., 2016).

ii. Recolección de evidencia digital web

Con respecto a la recolección de la evidencia digital, en varios estudios (Ohana y Shashidhar, 2013; Said et al., 2011) los autores analizan y recolectan evidencia digital en sesiones privadas; pese a que en este tipo de sesiones la cantidad de información que se almacena en el disco duro es mínima(Gupta y Mehtre, 2013; Nair y Ajeena, 2014), Por otro lado, Ohana y Shashidhar (2013) recolectan evidencia procedente de una sesión portable, analizando la memoria volátil y la red. En otros estudios (Gupta y Mehtre, 2013; Mirza, 2008; Sivaprasad y Jangale, 2012) se presentan recomendaciones para la recolección de evidencia web, estos estudios indican lugares frecuentes donde los investigadores forenses trabajan para buscar evidencia digital (por ejemplo, registro Windows, carpeta AppData, log de eventos del sistema, archivos temporales).

Los autores Raju y Geethakumari (2016) proponen un modelo iterativo para investigación forense en la nube, que considera la preservación y recolección de artefactos hasta que se determine un incidente; para luego dejar la evidencia digital lista para la investigación; sin embargo, los autores no presentan guías específicas para evidencia digital que proviene de entornos web en el lado del cliente. Otro aspecto importante a considerar según Lee et al., (2005) es la volatilidad de la evidencia, en el artículo se recomienda que se maneje el siguiente orden de volatilidad para recolectar la evidencia: 1) Registros caché, 2) Tablas de enrutamiento, 3) ARP caché, 4) Tabla de procesos,5) Memoria, 6) Archivos temporales, 7) Disco, 8) Registros remotos, 9) Información de monitoreo que es importante para el sistema en cuestión(configuraciones físicas

o lógicas, topologías de red, etc.); aunque este estudio no aborda de forma específica artefactos web. De la misma manera, Baca et al., (2013) recomiendan al levantar la evidencia realizar una imagen forense del disco, los autores emplearon “Integration Forensic tool EnCase” para realizar la imagen forense, montar la misma y crear los valores hash y sumas de verificación (checksums) de la evidencia.

Adicionalmente, posible automatizar los procesos de recolección de evidencia, en otros estudios los autores emplean la herramienta FTK para recolectar información sin alterar la evidencia web original (Mehreen y Aslam, 2015; Ohana y Shashidhar, 2013), por otro lado (Chen et al., 2015) analiza herramientas para aplicaciones en la nube y redes sociales incluyendo tomando en cuenta el uso de sesiones privadas. También existen herramientas interesantes al momento de recolectar la información por ejemplo WinHex que permite recuperar archivos eliminados o WinSpy para localizar actividades en Internet; estas junto con otras herramientas son presentadas por Sivaprasad y Jangale (2012). Por su parte Chow et al., (2005) integra desde esta fase métodos para preservar los datos, proponiendo un sistema de archivos de integridad basado en valores hash para analizar los archivos (Chow et al., 2005).

iii. Preservación de la evidencia digital web

Acerca de la preservación de la evidencia digital que se ha recolectado, Lee et al., (2005) y Farina et al., (2015), recomiendan que la evidencia debe ser recolectada teniendo en cuenta su volatilidad para perder la menor cantidad de información posible y preservarla adecuadamente. Además en los estudios de Jang y Kwak, (2015) y Matsumoto y Sakurai, (2014) los autores recomiendan usar y mantener la evidencia en imágenes forenses fieles a la original antes de proceder con el análisis. Adicionalmente Jang y Kwak, (2015) recomienda grabar en video la recolección y tratamiento de la evidencia para garantizar la integridad de esta durante cada proceso y que exista más de una persona durante la recolección de la evidencia. Sivaprasad y Jangale (2012), presentan otras técnicas para preservar evidencia digital; como asignar códigos hash para poder verificar la integridad de la información almacenada, las técnicas que se presentan están basadas en la publicación del RFC 3227.

Otra propuesta para la preservación de la evidencia digital es la publicada por Lee et al., (2005), que sugiere un proceso basado en tres pasos: 1) Un esquema que publique valores hash y checksums de evidencia digital, 2) Un sistema que gestione la evidencia digital para crear un valor MAC (Message Authentication Code) y registrar todo en el registro de cadena de custodia 3) Un sistema de autenticación en línea basado en firma digital. También resulta de mucha utilidad extraer y examinar los valores de checksums y hash de la evidencia original para su comparación con la imagen (Mehreen y Aslam, 2015).

Por otro lado Saleem, Popov y Dahman (2011) presenta directrices para evaluar los métodos de aseguramiento o preservación de la evidencia digital, los criterios de evaluación de los métodos son: propiedades de seguridad (integridad, confidencialidad, no repudio), identificación y autenticación, precisión, funcionalidad, fortaleza de los mecanismos, evaluación de vulnerabilidades, facilidad de uso y eficiencia computacional.

iv. Análisis y Reporte

Con relación al análisis automatizado, los autores Mahaju y Atkison (2017), toman en cuenta herramientas funcionales únicamente con el navegador Firefox. Ellos realizan una comparativa independiente de plataforma entre herramientas forenses que simplificaran el análisis de evidencia digital (por ejemplo, NetAnalisis V2, FoxAnalisis V1.6.0, PaswordFox, Browser History Examiner, Mz History Viewer) para analizar características como rendimiento, portabilidad, simplicidad, velocidad, clasificación de las actividades del usuario, memoria, consumo del CPU. Por otro lado Nalawade et al., (2016) examina herramientas para análisis de evidencia que dejan los navegadores web utilizando el Sistema operativo Windows. Chown et al., (2005) describe el sistema “Digital Evidence Search Kit” (DESK), el cual es utilizado por la policía de Hong Kong mediante el cual es posible ilustrar características de una herramienta integra para manejar la evidencia digital.

En otro estudio (Oh et al., 2011), los autores presentan herramientas para analizar diferentes artefactos de navegadores; por ejemplo, se presenta Pasco Web Historian 1.3, el cual puede ser utilizado en Internet Explorer, Firefox, Safari u Opera para analizar sus historiales y el archivos index.dat; también Chrome Alaysis 1.0 se utiliza con el navegador Chrome para analizar cookies, historiales, procesos de Windows, otra herramienta recomendada para el análisis de evidencia web es Internet Evidence Finder v4.0 (Marturana et al., 2012).

Luego del análisis, Oh et al., (2011) establece que el investigador debe generar un reporte basado en la información más relevante y sus afirmaciones, registrando la evidencia que soporta las conjeturas realizadas.

Durante esta revisión también se ha encontrado que la mayor parte de estudios son evaluados y probados mediante casos de estudio o pruebas de concepto (Baca et al., 2013; Marturana et al., 2012; Oh et al., 2011; Ohana y Shashidhar, 2013). Además, la tendencia a futuro para los proveedores de las aplicaciones web o SaaS es la de brindar el servicio forense en sus aplicativos, en el caso de la computación en la nube este servicio se denomina FaaS (Forensic as a Service) (Choo et al., 2017).

v. Revisión de estándares internacionales

Los estudios seleccionados para solventar la pregunta de investigación RQ5 no proponen guías comunes en sus enfoques, tampoco están fuertemente ligados a herramientas ni poseen sus propias metodologías. Sin embargo, los estándares ISO pueden dar un mejor lineamiento que denotaría reducciones en los tiempos de investigación e implementación de herramientas, mejorando el proceso investigativo y obteniendo resultados claros y precisos; generando así métodos existentes hacia un proceso forense viable.

Además, a continuación, se presenta una revisión de como las regulaciones pueden ser incluidas para el correcto manejo de evidencia digital en diferentes entornos (web, cloud, etc.). Se inicia del hecho que la información debe ser protegida por los mismos sistemas que la procesan, éste es uno de los principales objetivos en un proceso investigativo. Para poder manejar toda la información y para que esta pueda ser empleada en un proceso judicial, es necesario tener métodos donde cada proceso esté documentado con bases de seguridad y análisis de riesgos. Para acatar con todos los requerimientos existen estándares que guían el manejo de la seguridad de la información, identificación de riesgos e implementación de controles de seguridad (Council, 2013).

La ISO/IEC 27000 es un conjunto de estándares que incluyen las mejores prácticas en el área de la seguridad de la información. Dentro de esta familia de estándares, existen estándares particulares que pueden ser articulados a las prácticas de la informática forense. La Tabla 3.9, muestra los estándares que se pueden relacionar con las prácticas forenses.

Tabla 3.9: Estudios que pueden aportar a las prácticas forenses.

ISO/IEC 27041 (2015)	Orientación para asegurar la idoneidad y adecuación del método de investigación del incidente.
ISO/IEC 27037 (2012)	Directrices para identificación, recolección, adquisición y preservación de la evidencia digital.
ISO/IEC 27017 (2015)	Código de buenas prácticas para el control de la seguridad de la información para servicios en la nube.
ISO/IEC 27050 (2017)	Código de práctica para el descubrimiento electrónico.
ISO/IEC 27042 (2015)	Directrices para el análisis e interpretación de la evidencia digital.

La ISO/IEC 27041 (2015), es de gran utilidad durante la selección de la metodología para el análisis de la evidencia, está metodología seleccionada puede ser utilizada para actividades similares (Jaromír Veber y Klíma, 2014). Considerando que la ISO/IEC 27037 (2012) y 27042 (2015) se complementan describiendo 7 actividades principales en una investigación forense, las cuales son: i) planeación, ii) preparación, iii) respuesta, iv) identificación, recolección, preservación, v) análisis, vi) reporte y vii) cierre (Miranda Lopez et al., 2016). Por su parte el estándar ISO/IEC 27037 (2012), no promueve el uso de herramientas particulares; sin embargo, presenta tareas para las 7 actividades planteadas y el personal capacitado relacionado con la investigación.

Continuando con las actividades dadas por los estándares, el primer y segundo paso son utilizados por investigadores y profesionales. El tercer paso es para determinar el alcance del incidente, en el caso de un entorno cloud, lo primero es verificar la existencia de leyes de acuerdo con la jurisdicción.

En el cuarto paso, se recoleta la información, configuración de la red y relacionada al sistema. En caso de existir problemas en el análisis, los investigadores deben recurrir a los proveedores para un trabajo en conjunto tomando en cuenta la seguridad de los datos que se describen en los estándares. Para completar la ISO/IEC 27037 (2012), para entornos cloud, la ISO/IEC 27017 (2015), es utilizada, la cual describe servicios particulares de este paradigma; donde se aconseja a los clientes verificar que los proveedores cumplan con el estándar (Council, 2013). En el mismo paso, la recolección de los datos es maximizada, pero en una infraestructura cloud es larga y cambiante; por lo que esto puede generar conflictos cuando los profesionales requieren extraer información, por lo que es de gran utilidad determinar qué información es valiosa y usar herramientas y técnicas forenses para el proceso. Para completar este paso la ISO/IEC 27050 (2017). es aplicada, puesto que este estándar describe el proceso de descubrir la información en dispositivos móviles como computadores portátiles, es muy empleado por investigadores como por personas no técnicas.

El quinto paso está enfocado en asegurar la completa extracción de evidencia a través de procedimientos de adquisición. Ahora si el procedimiento se encuentra en el contexto de un ambiente cloud; surge un problema relacionado a la capacidad de almacenamiento, puesto que entornos como este y de tener acceso a la información las cantidades de información pueden estar en rangos de terabytes (Miranda Lopez et al., 2016). En estos casos, es recomendable emplear técnicas de minería de datos para la extracción de los mismos de acuerdo a su importancia. Finalmente, la preservación de la evidencia no debe ser contaminada, los investigadores deben garantizar que la evidencia no ha sido alterada. Entonces, los profesionales deben realizar una copia de la evidencia

original, la misma que no debe ser tratada ni manipulada para mantener su integridad.

Como es conocido, la computación en la nube ha avanzado; existiendo algunos proveedores de computación en la nube brindar servicios de almacenamientos avanzados; permitiendo a los usuarios encriptar su información, la ISO/IEC 27017 (2015), propone que los clientes de los servicios en la nube deben limitar sus datos de forma que, si un empleado del proveedor obtenga acceso, este no pueda usar estos datos. El sexto paso es un reporte del proceso entero y de lo encontrado durante la investigación forense. En este paso la ISO/IEC 27042 (2015) y la 27043 (2015), sugieren no solo presentar el análisis de la evidencia sino también la interpretación de los resultados, escribiendo un reporte, posterior al reporte de resultados el investigador puede dar por cerrada la investigación (Jaromír Veber y Klima, 2015; Jaromír Veber y Klíma, 2014).

Finalmente, Veber y Smunty, explican que la ISO 27037 no es enteramente práctica, pero empleándola en conjunto con los otros estándares mencionados pueden ser una gran guía para una investigación forense, así como para mejorar métodos y herramientas empleadas. Otro punto importante es que los estándares no solo ayudan a los investigadores, también puede servir como una base para los expertos judiciales para que los mismos puedan entender lo planteado en el reporte final.

En la Figura 3.2 Se puede apreciar la intersección del número estudios relacionados entre los principales criterios de extracción relacionados de forma principal con los estándares. De acuerdo al análisis en cuanto a los estándares, existen 2 estudios que afirman que toman en cuenta la ISO/IEC 27037 con respecto a métodos de autenticación. Además, se puede apreciar una que el estándar más empleado o citado en esta revisión de estándares es la ISO/IEC 27037, esto puede atribuirse a que es la más antigua en el grupo de estándares estudiados para esta revisión.

Figura 3.2: Relación de los criterios de extracción con la revisión de estándares.

Al término del presente capítulo las preguntas de investigación planteadas:

RQ1: ¿Qué tipo de evidencia web se puede encontrar en la computadora del cliente?

RQ2: ¿En qué lugar de la computadora del cliente se puede encontrar evidencia digital de entornos web?

RQ3: ¿Qué herramientas se pueden utilizar para automatizar el manejo de evidencia web?

RQ4: ¿Cómo preservar la evidencia digital para garantizar su integridad?

RQ5: ¿Cómo los estándares están siendo empleados en el manejo de la evidencia digital?

Han sido respondidas en los diferentes apartados del reporte de resultados de revisión de literatura.

RQ1, ha sido respondida en el apartado de identificación; donde se han detallado varios artefactos web que pueden ser encontrados en el equipo local; como cachés, cookies o archivos temporales provenientes de entornos web que son dejados en el lado del cliente con información de las interacciones entre el cliente y el sitio web.

RQ2 de la misma forma, fue respondida en el apartado de identificación; ahí se ha verificado que las aplicaciones dejan evidencia proveniente de la web en diferentes directorios de los sistemas operativos que deben ser localizados para recolectar los artefactos (como la carpeta AppData en Windows almacena los directorios donde aplicaciones como Google Chrome almacenan su caché).

Por otra parte, RQ3, ha sido solventada en los apartados de recolección, preservación y análisis, pues se ha detallado varias herramientas que permiten automatizar procesos de recolección, generar métodos de integridad para la evidencia digital y también herramientas que facilitan la interpretación de la evidencia en la fase de análisis.

RQ4, esta pregunta se ve contestada en el apartado de preservación, identificando varios métodos, como funciones hash, firmas digitales, etc., que emplean los expertos para preservar evidencia digital (incluida la proveniente de entornos web).

Finalmente, RQ5, está pregunta de investigación ha sido solventada en el apartado de revisión de los estándares internacionales; está revisión ha sido enfocada en la familia de la ISO/IEC 27000, que proveen directrices en la seguridad de la información.

Como conclusión de esta revisión de literatura se puede decir que si bien existen estudios que recolectan buenas prácticas para el manejo de evidencia digital proveniente de entornos web, estos en su gran mayoría presentan soluciones específicas o no incluyen todas las etapas de una investigación forense. Por lo tanto, este trabajo de investigación busca proponer una metodología que permita a los investigadores manejar la evidencia digital proveniente de entornos web durante todas las etapas de la investigación; considerando recomendaciones de estándares internacionales.

Capítulo 4. Metodología Propuesta

De acuerdo con Lee et al. (2005) y las recomendaciones de los estándares ISO/IEC 27037 (2012) y 27042 (2015), un proceso de informática forense consiste básicamente en los siguientes pasos: (i) Preparación, (ii) Adquisición, (iii) Preservación, (iv) Examinación y análisis, (v) Reporte. Este trabajo de titulación propone una metodología alineada con estas fases clave de toda investigación forense (Lee et al., 2005), pero orientada a evidencia digital proveniente de entornos web del lado del cliente (ordenador) y la incorporación de las recomendaciones de estándares internacionales (i.e., ISO/IEC 27037, ISO/IEC 27042). Para esta metodología se recomienda que el dispositivo objeto de la investigación fue recolectado de acuerdo con las recomendaciones del estándar ISO/IEC 27037 (2012), con la finalidad de resguardar la integridad de las posibles evidencias digitales.

Los pasos que describen la metodología propuesta son: i) Identificación, ii) Recolección, iii) Preservación, iv) Análisis y v) Presentación. En la Figura 4.1, se muestra la metodología propuesta junto con las entradas y salidas de cada fase; además se hace referencia a las fases en las que se consideran las recomendaciones de los estándares internacionales (i.e., ISO/IEC 27037 y 27042), la cual ha sido ilustrada utilizando SPEM 2.0 (Software Process Engineering Metamodel) («OMG», 2008).

En las siguientes subsecciones se describe cada uno de las fases y actividades correspondientes a la metodología. De esta manera, se guía al lector durante cada una de las actividades propuestas en esta metodología, tomando en cuenta las sugerencias propuestas en estándares internacionales.

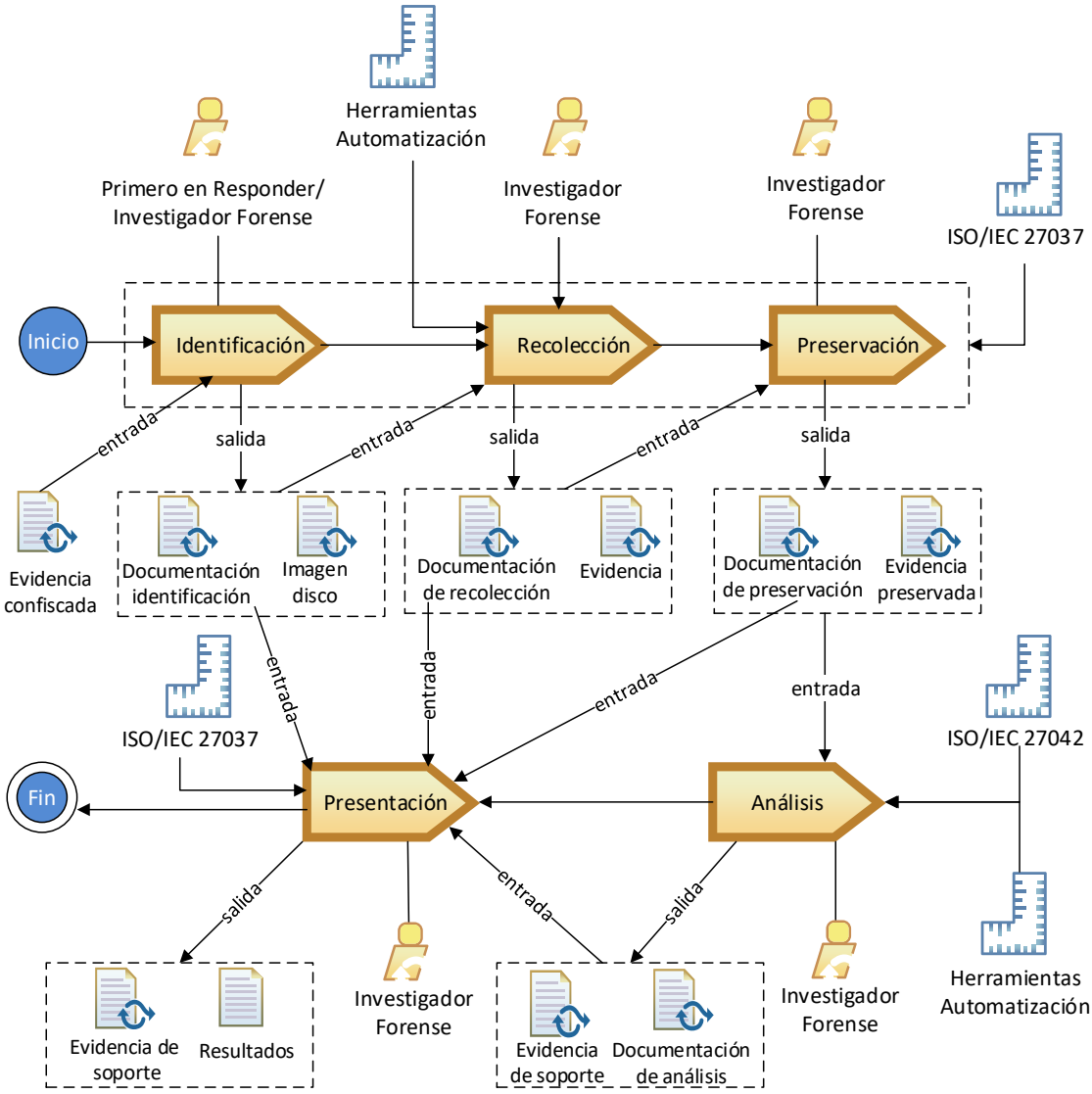


Figura 4.1: Metodología Propuesta.

4. 1. Identificación de Evidencia Web

Esta es la primera fase de la metodología propuesta, realizada por el investigador forense, para lo cual es necesario que se entregue al investigador, el equipo identificado en el lado del cliente que interactuó con algún servidor web. El equipo puede estar en funcionamiento o pudo haber sido debidamente confiscado y entregado al investigador.

Antes de proceder a la recolección o adquisición de los datos es necesario que el equipo esté desconectado de cualquier red, también las marcas identificadoras del ordenador deben ser registradas y documentadas de acuerdo con la ISO/IEC 27037 (2012).

A continuación, se describen las tareas y sugerencias a considerar durante esta fase. La dificultad de este paso radica en garantizar la integridad de la cadena de custodia de la evidencia (Baca et al., 2013). Una vista del flujo de tareas y actividades de esta fase se muestran en la Figura 4.2.

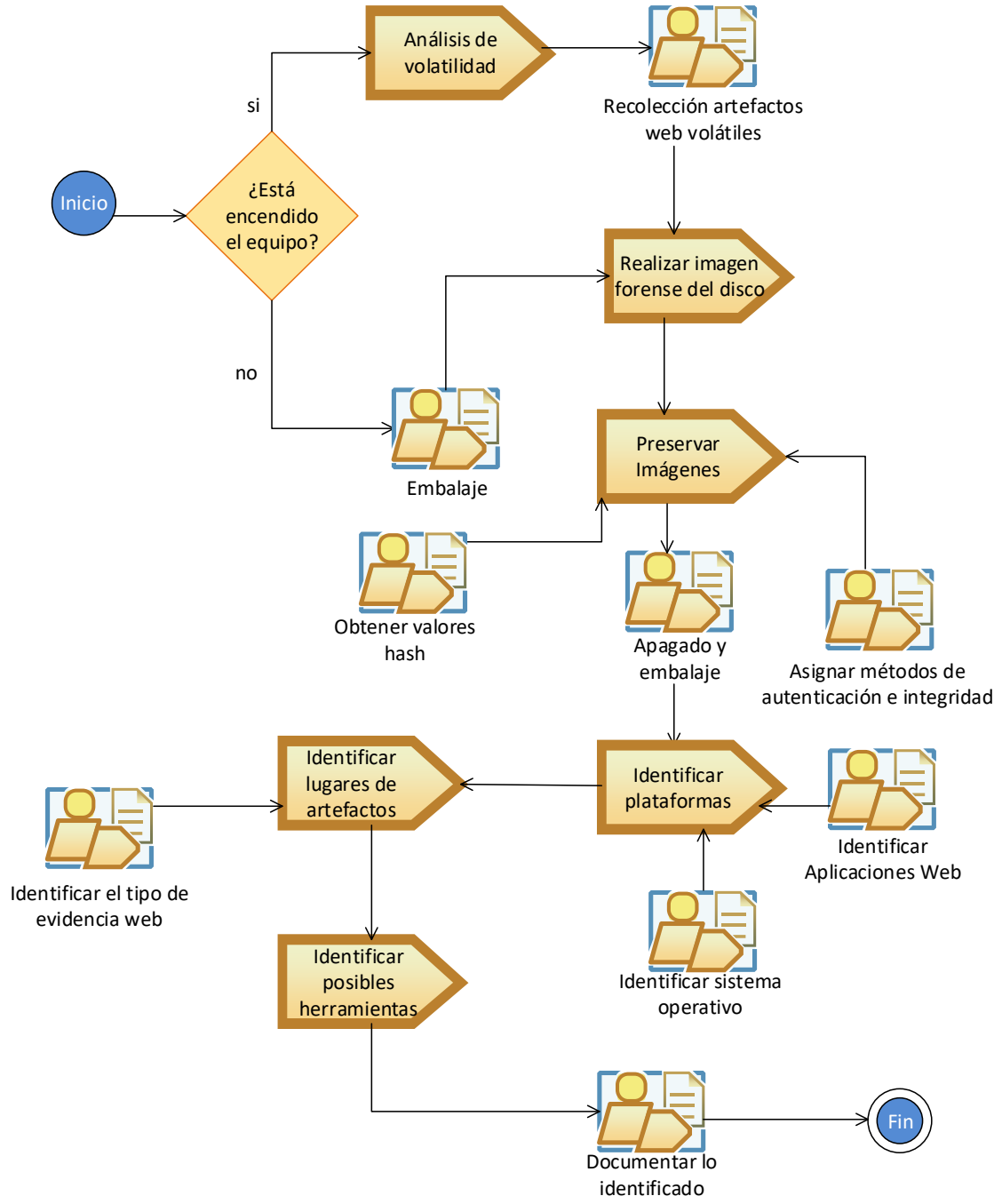


Figura 4.2: Flujo de tareas y actividades de la fase de identificación

4.1.1 Verificación del Estado del Ordenador (on/off)

Puede existir el caso en el que se tenga realizar una investigación en vivo, es decir que el sistema siga encendido; en ese caso se debe considerar la volatilidad de la evidencia para evitar perder información valiosa del ordenador cuando este se apague y capturar la misma (Lee et al., 2005). Información que pueda estar almacenada en memoria primaria o memoria de carácter volátil. En algunos casos por la complejidad de este proceso es recomendable que el proceso lo realice un técnico forense.

En caso de que el monitor este encendido, se debe capturar los procesos que se están ejecutando de ser el caso acorde a la ISO/IEC 27037 (2012). Y realizar el siguiente paso de inmediato para evitar perder la mayor cantidad de información.

Pero en el caso que el equipo este apagado, no se necesita un análisis de volatilidad, simplemente se recomienda retirar el dispositivo de almacenamiento del ordenador y un correcto embalaje de acuerdo con la ISO/IEC 27037 (2012), luego de esto se puede proceder a realizar la imagen del disco.

4.1.2 Análisis de volatilidad

El investigador debe establecer prioridades en la evidencia; además, establecer la volatilidad de la misma puede ser sustancial en una investigación puesto que se reduce la posibilidad de perder evidencia importante en la investigación (Lee et al., 2005), el orden de volatilidad considerado para la investigación debe ser documentado. Si bien Lee et al., (2005), establece una escala de prioridades de acuerdo con el RFC 3227 de 7 niveles, para la presente guía se ha considerado los elementos que contienen artefactos procedentes de sitios web en los siguientes niveles de prioridad:

1. Registros, caché.
2. Memoria.
3. Sistemas de archivos temporales.
4. Disco.

Conforme se recomienda dicha escala de volatilidad, luego de analizar y capturar los datos sensibles (considerando sugerencias de preservación), la ISO/IEC 27037 (2012), recomienda verificar si los datos que se mantienen en el ordenador se mantienen de forma estable; de ser el caso se procede a apagar el sistema de forma normal. Pero, de no ser el caso y los datos estar almacenados en el ordenador, éstos corren peligro (por ejemplo, se está

ejecutando un proceso de borrado de archivos), se debe retirar de inmediato la fuente de energía del equipo.

Se debe bloquear la escritura mientras se realiza la adquisición de cualquier información del dispositivo objeto de la investigación.

En caso de que se esté desarrollando una situación que ponga en alto riesgo el dispositivo de almacenamiento del equipo, se recomienda emplear herramientas específicas para la adquisición de los artefactos web del ordenador. Es posible que el investigador cree sus propias herramientas enfocándose a los artefactos web más relevantes (si se tiene algún indicio), logrando una recolección de estos en menor tiempo.

4.1.3 Realizar Imágenes forenses.

Es recomendable realizar copias bit a bit de la evidencia digital que almacenan los equipos, para poder trabajar con las mismas asegurando la integridad de la evidencia original. Las imágenes forenses ayudan a los investigadores a capturar evidencia o realizar análisis sin alterar la evidencia original (Jang y Kwak, 2015; Lee et al., 2005).

Otra acción recomendable en este punto es extraer los valores hash de la o las imágenes para comparar su integridad en todo momento y poder asegurar la integridad de la evidencia a medida que esta es analizada.

Es recomendable utilizar una herramienta debidamente validada para este proceso acorde con la ISO/IEC 27037 (2012) y ISO/IEC 27042 (2015).

4.1.4 Preservar imágenes forenses

Al momento de almacenar las imágenes digitales es recomendable garantizar que solo las personas que deben tengan acceso a la misma, por lo que es recomendable utilizar métodos de autenticación, integridad (por ejemplo: firma digital, valores hash, claves primarias).

4.1.5 Identificar plataformas relacionadas

Algo primordial que se debe realizar previo a la recolección y análisis es identificar las diferentes plataformas, aplicaciones que se utilizaron en el caso; las actividades primordiales de identificación que se recomiendan son:

- Identificar el sistema operativo.
- Identificar de ser posible que aplicación web es el objeto de la investigación.

- De ser posible identificar que navegadores web o aplicaciones de escritorio pudieron ser empleadas.

Estas actividades son importantes para reducir el campo en donde la evidencia web puede ser encontrada. Además con esta información se facilita el trabajo para determinar las herramientas apropiadas para la investigación, esto por las dependencias de plataforma de las herramientas (Mahaju y Atkison, 2017; Nalawade et al., 2016).

4.1.6 Identificar lugares de artefactos web

Esta actividad se basa en identificar las posibles direcciones dentro del sistema operativo donde las aplicaciones web almacenan la información que manejan, por ejemplo, archivos temporales o logs de actividades. Esto puede ser útil para identificar si las herramientas de automatización son efectivas, es decir si las mismas examinan estos lugares, y en el caso de que no existan herramientas que examinen estos lugares, la búsqueda deber ser manual o las herramientas podrían ser creadas por el investigador. A continuación, se guía al lector en los posibles lugares en donde los artefactos web pueden estar almacenados considerando los principales medios para la interacción con aplicaciones web:

- Navegadores: Se debe verificar la ruta en la que el navegador almacena sus artefactos web dependiendo del sistema operativo, los artefactos que se pueden encontrar son: cookies, cachés de navegación, historiales de navegación, historiales de accesos, cuentas, etc.
- Aplicaciones de escritorio: Se verifica el directorio de la aplicación, por lo general las aplicaciones de escritorio utilizan archivos temporales, o generan logs de sus actividades.

4.1.7 Identificar posibles herramientas

Con la información que se ha recopilado, es posible identificar que herramientas que pueden ser útiles para automatizar y facilitar el proceso de recolección, análisis y preservación de la evidencia. Considerando herramientas compatibles con las diferentes plataformas. Como se mencionó antes, si se emplean herramientas para automatizar ciertos procesos, es imperante verificar la validez de estas.

La identificación correcta de estas herramientas puede denotar en una mejora de tiempos cuando ésta es realizada de manera correcta.

4.1.8 Identificar si existe software de borrado de archivos

Esta actividad es fundamental y recomendada por la ISO 27037 (2012), verificar si en el ordenador existe algún programa que efectúe el proceso borrado de archivos (por ejemplo, Ccleaner). Esto con la finalidad de tener una idea de las posibles actividades que el usuario pudo realizar.

Al finalizar esta fase se debe obtener:

- Documentación de toda la información identificada en esta fase.
- Imágenes forenses.
- Reporte de la cadena de custodia, debidamente actualizado.

4.2. Recolección de la Evidencia Web

Una vez que se han identificado los indicios iniciales, es necesario recolectar la evidencia web que puede ser evidencia potencial en la investigación forense. La entrada para esta fase son as imágenes forenses creadas en la fase anterior. En la Figura 4.3 se muestran las tareas y actividades de la fase de recolección de la evidencia digital realizadas por el investigador forense. A continuación, se describen las actividades recomendadas en esta fase luego de comprobar la integridad de las imágenes.

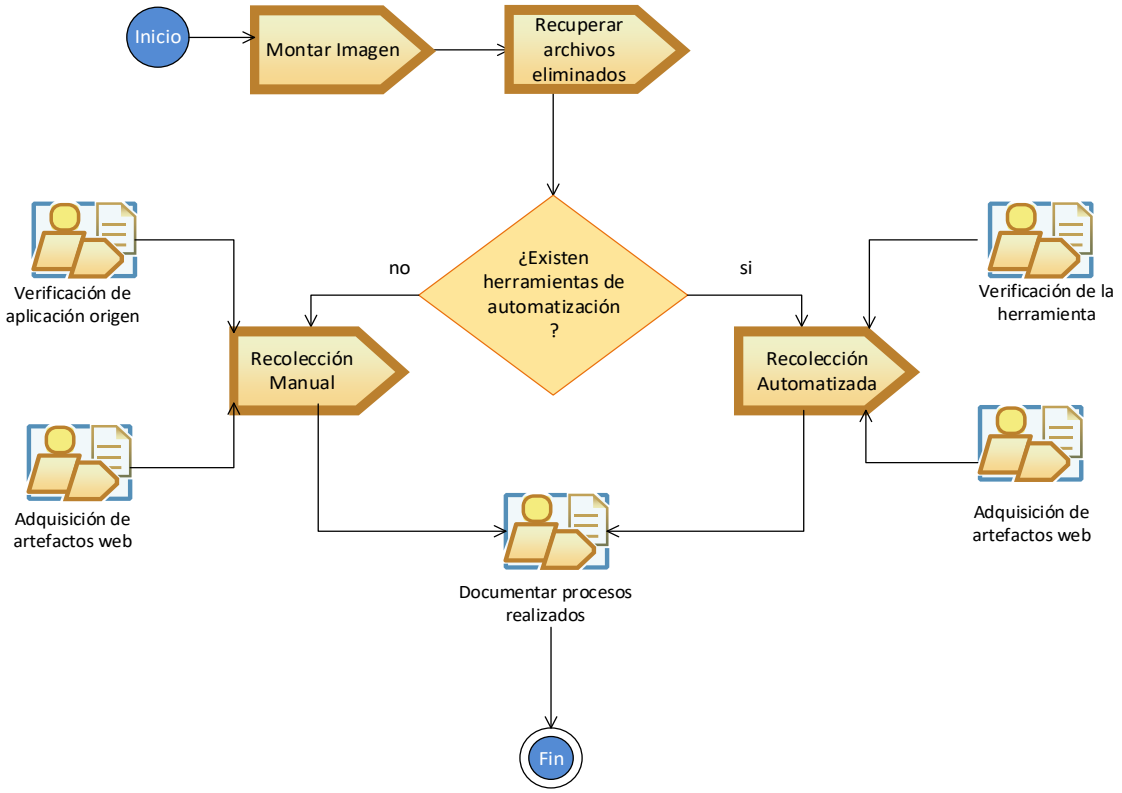


Figura 4.3: Flujo de tareas y actividades de la fase de recolección.

4.2.1 Montar Imagen

Esto se realiza para establecer el estado en el cual equipo fue encontrado, previo a montar la imagen se sugiere revisar las sumas de verificación para tener seguridad que la evidencia con la que se trabaja es integra.

Adicionalmente, de acuerdo con la recomendación de la ISO/IEC 27037 y 27042 se debe bloquear cualquier tipo de escritura en la información objeto de nuestra investigación.

4.2.2 Recuperar archivos eliminados

Previo a recolectar la información que se encuentra en el sistema operativo, se intenta una recuperación de los archivos que fueron eliminados del ordenador e identificar posible evidencia web dentro de los mismos (Oh et al., 2011).

4.2.3 Recolectar artefactos web

Varios autores (Chen et al., 2015; Marturana et al., 2012; Oh et al., 2011) emplean herramientas que automatizan este proceso, pero de no existir una herramienta ya sea por la dependencia del sistema operativo o la dependencia de las aplicaciones; el investigador debe realizar una recolección manual de los artefactos web que pudieron ser dejados por la aplicación Web o SaaS, esto provoca una carga adicional al investigador debido al incremento de tiempo de dedicación para esta tarea.

Es adecuado asegurarse que los logs, archivos temporales, archivos que la aplicación utilizó sean recolectados. En caso de que la aplicación que se utilizó para la interacción hubiera sido un navegador (por ejemplo, Firefox, Google Chrome), también se debe asegurar que se recolecto el historial, registros de favoritos, historiales de descargas, caché y cookies del navegador.

De no encontrar mayores artefactos web, es posible que se haya utilizado una sesión privada o portable, en tales casos la información que el ordenador conserva es mínima, por lo que es recomendable analizar los archivos de las extensiones de los navegadores pues las mismas no poseen modo incógnito o acudir a la memoria RAM.

En algunos entornos es necesario realizar adquisiciones parciales, ya sea porque la cantidad de datos es alta, solo una parte de los datos es relevante, etc. Pero cuando se toma esta decisión la norma ISO/IEC 27037 (2012) recomienda estos aspectos entre otros: identificar las carpetas, archivos o cualquier opción de sistema propietario relevantes para adquirir los datos deseados, para luego realizar la adquisición lógica de esos datos identificados. O también es

recomendable investigar y emplear técnicas de minería de datos (Miranda Lopez et al., 2016).

Al culminar las actividades de esta fase las salidas de esta fase se describen a continuación:

- Documentación de la evidencia web recolectada, su procedencia y el tipo de esta.
- Evidencia digital

Una recomendación importante provista por la ISO/IEC 27037 al momento de recolectar o adquirir la evidencia digital, es balancear de acuerdo con: las circunstancias, costo, tiempo, recursos disponibles y prioridades.

4.3. Preservación de Evidencia Web.

Al iniciar esta fase es necesario que la entrada de la misma sea la evidencia web recolectada, la cual debe ser debidamente preservada para continuar con las investigaciones. En la figura 4.4 se muestran el flujo de tareas y actividades de esta fase. Las cuales se describen a continuación. De no existir ninguna restricción, los métodos de preservación son definidos y aplicados por el investigador forense.

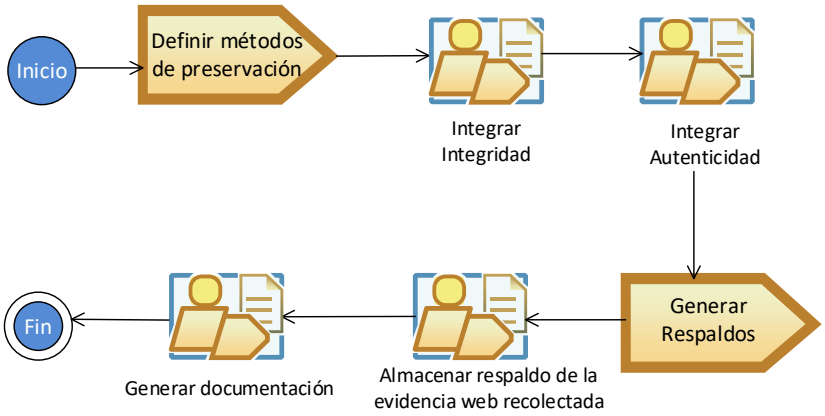


Figura 4.4: Flujo de tareas y actividades de la fase de preservación

4.3.1 Definir métodos de preservación

Se deben definir métodos para garantizar autenticación e integridad sobre la evidencia recolectada. Puesto que es importante que solo personal autorizado tenga acceso a la evidencia web y que la evidencia se mantenga íntegra durante toda la investigación. Para cumplir con estas características obligatorias en una investigación forense se puede utilizar claves de acceso, verificaciones de sumas (checksums), firmas digitales o valores hash (Lee et al., 2005).

Se debe utilizar una función de verificación, para proveer evidencia de tal forma que las copias sean equivalentes a la original. Además, es aconsejable ligar la evidencia con el investigador forense utilizando sistemas biométricos, formas digitales fotografía de acuerdo con la ISO/IEC 27037 (2012).

4.3.2 Generar Respaldos.

Es recomendable mantener la evidencia que se ha recolectado respaldada y preservada con los métodos revisados, para que si existe alguna alteración de la evidencia con la que se está trabajando se pueda recurrir a él. El respaldo (pueden ser imágenes) debe mantener una identificación del dispositivo de almacenamiento. Además, es importante manejar una cadena de custodia de éste.

Al finalizar las actividades de esta fase se obtiene:

- La evidencia web debidamente preservada.
- La documentación de esta etapa contiene los métodos empleados para la preservación de la evidencia web y los dispositivos donde se encuentra la evidencia web con sus identificadores.

4.4. Análisis de evidencia digital de la web

Para realizar esta fase se debe recibir la evidencia web preservada, y previo a las actividades concernientes al análisis se realiza el proceso de autenticación y la verificación de que la evidencia digital se mantenga integra. De no estar la evidencia integra se debe recurrir a la copia almacenada de la evidencia en el apartado de preservación. A continuación, se describen las actividades a considerar en durante esta fase. En la Figura 4.5 se muestra el flujo de tareas y actividades de la dase de análisis que son ejecutadas por el investigador forense.

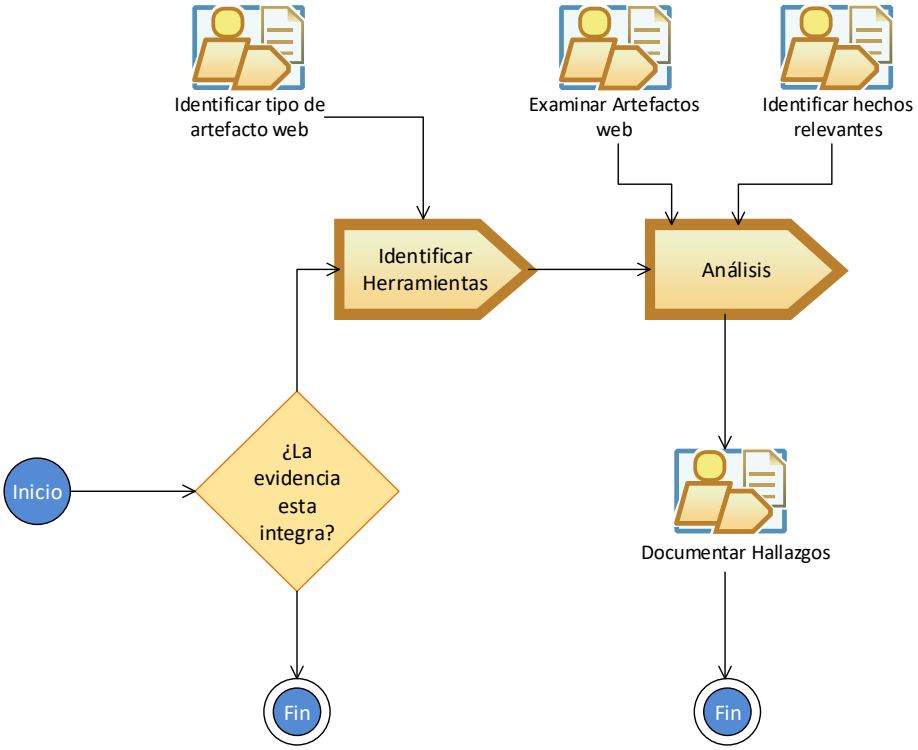


Figura 4.5: Flujo de tareas y actividades de la fase de análisis.

4.4.1 Identificar herramientas

Es necesario seleccionar las herramientas, adicionales a la fase de identificación, que permitan la interpretación de los artefactos web recolectados. Estas herramientas facilitan el análisis, porque clasifican la evidencia web dependiendo del lugar de dónde provienen y la presentan en formatos legibles. De no poseer herramientas que faciliten el análisis, se debe realizar un análisis manual, identificando los archivos y sus respectivos formatos para poderlos interpretar. En esta fase se recomienda al investigador, identificar herramientas adicionales, que no pudieron ser identificadas en la primera fase de la metodología.

4.4.2 Análisis

Se debe documentar lo que se encontró en la evidencia web recolectada, siempre que sea relevante para la investigación. Algunas veces las herramientas proveen un reporte fácil de interpretar y que permiten identificar sucesos importantes dentro del sistema (Mehreen y Aslam, 2015), aunque en otras ocasiones puede ser necesario un análisis manual y detallado sobre la evidencia web, puesto a que esas herramientas no siempre presentan la evidencia completa lo que genera que el investigador requiera el uso de más de una herramienta.

A continuación, se presenta el tipo de información que se puede encontrar como evidencia digital procedente de sitios web previamente indicados:

- Cachés: Se puede verificar imágenes, gifs, texto, cuentas de correos electrónicos.
- Cookies: Se puede verificar indicios de descargas, accesos a sitios web, entre otros.
- Historiales: Existen diferentes tipos de historiales:
    - Historiales de navegación: Los sitios web visitados por el cliente.
    - Historiales de Descargas: Elementos descargados de la web.
    - Otros: Dependiendo la aplicación pueden existir historiales de accesos, historiales de búsquedas entre otros.
- RAM: Dependiendo la herramienta que se emplee para interpretar la información, es posible encontrar procesos del sistema, parte de las cachés, imágenes completas o fragmentadas.
- Archivos temporales: Es posible encontrar archivos XMLs con datos de la aplicación web, imágenes, entre otros.
- Logs: Se puede verificar las actividades que han sido realizadas por el cliente en la aplicación.

Aparte de estos artefactos comunes en las aplicaciones web, algunas poseen otros archivos que contienen datos y metadatos relevantes, por lo que es importante analizar archivos adicionales en los directorios de la aplicación.

Además de estas sugerencias, de acuerdo con la ISO/IEC 27042 (2015), se recomienda al investigador documentar sus interpretaciones para incluirlas posteriormente al reporte final. Este proceso será de ayuda al momento de reconstruir las actividades realizadas para ser presentadas en un proceso judicial.

Al término de esta fase se tiene:

- Documentación de los resultados del análisis.
- Evidencia que apoye los resultados del análisis.

4.5. Presentación

La entrada de esta fase son la documentación de todas las etapas previas y la evidencia digital web preservada que soporte los resultados, el flujo de actividades recomendadas para el investigador forense se muestra en la Figura 4.6.

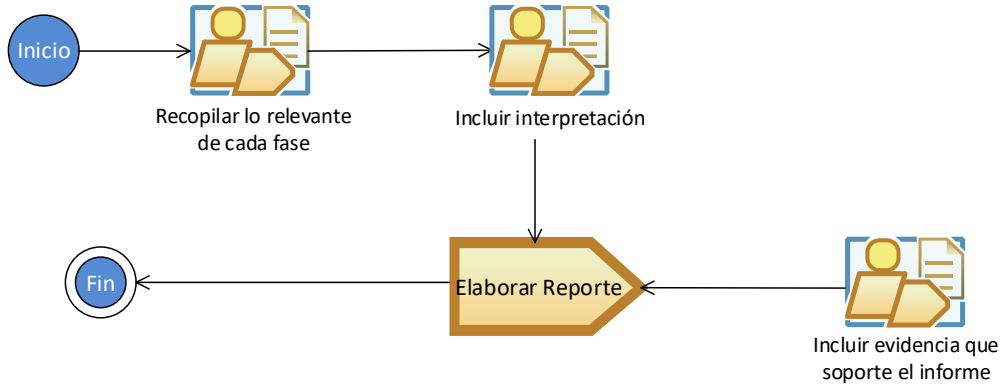


Figura 4.6: Flujo de actividades y tareas de la fase de presentación.

4.5.1 Elaborar Reporte

Los investigadores deben considerar la evidencia web relevante de toda la investigación. Lo cual depende del caso tratado y que hechos pueden ser relevantes para ayudar en un caso de investigación en la toma de decisiones (carga, descarga, modificación de recursos web). La evidencia digital relevante, según lo que se planteó en el objetivo del trabajo de titulación, es aquella que liga al usuario con las actividades realizadas en la interacción con aplicaciones en entornos web. También, se ha considerado como evidencia relevante, aquella que ayude a construir una línea del tiempo de las actividades del usuario (Oh et al., 2011). Además, es importante documentar en el reporte todos los procedimientos que fueron ejecutados durante la investigación.

Por último, el reporte debe ser fácil de entender para personas no técnicas, pero a la vez debe contener la evidencia digital que apoye los resultados obtenidos. Es importante conocer que todos los resultados obtenidos deben poder ser replicados por otros investigadores según la ISO/IEC 27037 (2012).

En este reporte, la evidencia web preservada debe ser adjuntada. Se debe asegurar que cuando la evidencia web va a ser presentada esta contenga métodos para permitir únicamente la lectura de esta y no permitir modificaciones.

Según la ISO/IEC 27037 (2012) en el reporte emitido por el investigador se debe considerar:

- Ningún detalle sea dejado fuera durante el proceso de identificación, recolección adquisición y preservación de la evidencia.
- El investigador debe considerar que el tiempo de los equipos, si están encendidos los mismos, este sincronizados con la hora válida, de ser posible comparar con una fuente de tiempo confiable y registrar aquello en el informe.

- Registrar todo lo visible por el monitor o pantalla del dispositivo; pudiendo ser programas activos, procesos, nombres de documentos abiertos. Estas capturas deben registrarse con una breve descripción.
- Cualquier movimiento con el ordenador debe ser registrado en la documentación.

Al culminar esta fase se debe obtener:

- Reporte Final
- Evidencia web de sustento

En el anexo B, el lector puede encontrar un informe pericial en el formato solicitado por la ley ecuatoriana.

5. Propuesta de Herramienta

En el presente capítulo se describe la herramienta desarrollada para automatizar y optimizar tiempos de recolección y preservación de la evidencia; incluyendo los objetivos de esta herramienta, el funcionamiento básico de la misma y los resultados obtenidos en las pruebas de funcionamiento ejecutadas. Esta herramienta será objeto de comparación con el software OS Forensics.

5.1 Motivación

En una investigación forense, de acuerdo con la ISO/IEC 27037 (2012), uno de los procedimientos fundamentales es la recolección de la evidencia digital. Dada la gran cantidad de información que un ordenador puede generar, es necesario que el investigador forense emplee herramientas que permitan recopilar los artefactos web relevantes para su investigación en el equipo local. De forma adicional se considera la volatilidad de la información; puede existir el caso en que el ordenador objeto de la investigación se encuentre en una situación de riesgo, y los datos alojados en su unidad de almacenamiento se vean comprometidos; por lo que se requiere una recolección rápida de los artefactos más importantes del equipo.

Bajo este contexto y motivación, se ve la necesidad de contar con una herramienta dirigida a la recolección y preservación de artefactos web específicos y relevantes para una investigación. En consecuencia, se ha planteado una herramienta que permita recopilar y preservar artefactos procedentes de dos de los navegadores web más utilizados en el mundo por los usuarios para interactuar con aplicaciones web: Google Chrome y Firefox Mozilla, en el sistema operativo Windows (Oh et al., 2011).

5.2 Objetivos

Para el desarrollo de la herramienta de automatización, se ha planteado el siguiente objetivo general:

Desarrollar una herramienta que automatice el proceso forense de recolección y preservación de la evidencia digital procedente de entornos web, para el caso particular de Firefox y Chrome.

Para alcanzar el objetivo principal de este apartado se han planteado 3 objetivos específicos que permitan cumplir dicho objetivo:

- Identificar el o los directorios donde los navegadores almacenan sus artefactos web.

- Recolectar los artefactos en un directorio que no altere el estado actual del disco.
- Asignar a los artefactos recolectados al menos un método para preservar su integridad.

5.3 Funcionamiento

La aplicación permite recolectar información directamente desde un dispositivo extraíble y salvaguardar la misma empleando funciones hash. El único requisito es conocer el directorio en donde la aplicación almacena sus archivos temporales, cachés, cookies, etc. Esto con la finalidad de verificar la posibilidad de reducir tiempos en la fase de recolección de la información.

Para facilitar el entendimiento, se han agrupado estas actividades en tres procesos principales que son: detección de directorios, recolección de artefactos y su preservación. Dentro de cada una de estas tareas principales existen procesos que deben ser realizados. En la Figura 5.1, se muestran las actividades y procesos principales que ejecuta la herramienta planteada.

La herramienta desarrollada sigue la siguiente rutina:

- Detecta si el directorio de la aplicación existe en el ordenador.
- Crea un directorio en el dispositivo extraíble para almacenar los artefactos de la aplicación.
- Extrae la posible evidencia digital procedente de entornos web.
- Calcula los valores hash para los archivos y directorios adquiridos.
- Los resultados son almacenados en un fichero de texto creado para cada aplicación, dentro del cual se tiene los directorios o archivos recolectados junto con sus valores hash.

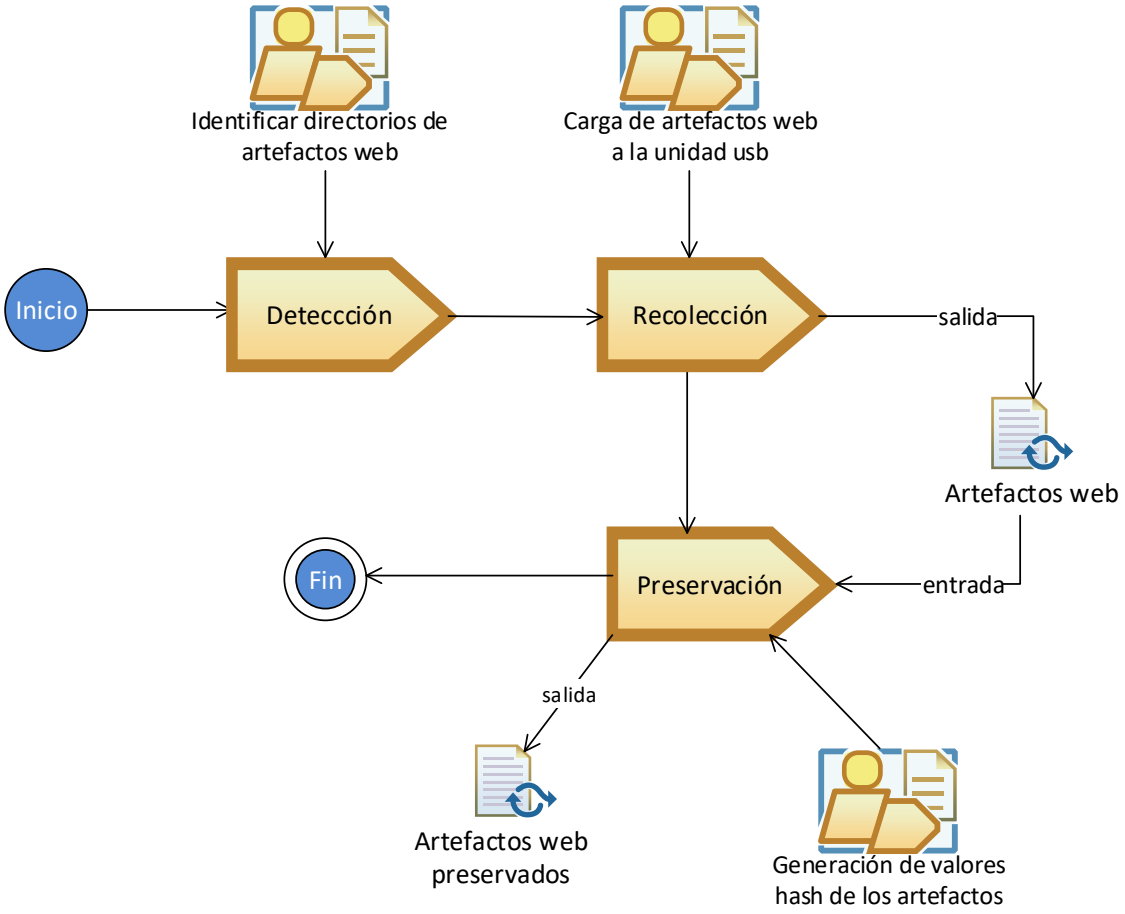


Figura 5.1: Tareas y procesos de la herramienta planteada.

5.4 Implementación

La aplicación ha sido desarrollada en Python, dentro del entorno de desarrollo Netbeans 8.2. A continuación se describe la implementación de las tareas y procesos señalados en la Figura 5.1. Los archivos del programa se pueden encontrar en el Anexo A.

5.4.1 Detección

Para detectar la existencia de una aplicación objeto de investigación, se requiere conocer previamente el o los directorios en los cuales aplicación almacena los artefactos web (e.g., cachés, cookies, archivos temporales, historiales). En la implementación actual se han desarrollado funciones que permiten al investigador obtener las ruta a los diferentes artefactos web, dentro del archivo funciones.py.

En la Figura 5.2, se muestra la función que devuelve el directorio de los artefactos web de Google Chrome; también se aprecian las funciones para

devolver los directorios donde Firefox Mozilla almacena sus cookies, historiales y la última función para la ruta del caché. La aplicación logra identificar las rutas en cualquier máquina con sistema operativo Windows en los idiomas español e inglés.

```
def definirChromePath():
    try:
        path=glob.glob("C:/Users/*/AppData/Local/Google/Chrome/User Data/Default")[0]
        return path
    except:
        import traceback
    # Print the stack traceback
        traceback.print_exc()
        return "0"
def definirMozillaPath():
    try:
        return glob.glob("C:/Users/*/AppData/Roaming/Mozilla/Firefox/Profiles/*")[0]
    except:
        return 0
def cacheMozillaPath():
    try:
        return glob.glob("C:\Users\*\AppData\Local\Mozilla\Firefox\Profiles\*")[0]
    except:
        return 0;
```

Figura 5.2: Funciones para devolver directorios de artefactos web.

Estas funciones son invocadas desde la ejecución principal del programa, para verificar la existencia de los diferentes aplicativos. De existir los directorios de las diferentes aplicaciones; es generado un directorio donde se almacenarán los artefactos web, como se muestra en la Figura 5.3.

```
pathChrome= funciones.definirChromePath()
tiempo_inicial = time()
if  os.path.exists(pathChrome):
    print "El navegador Google Chrome ha sido detectado"
    ch=1
    #Se crea un directorio en el dispositvo para almacenar sus artefactos
    if os.path.exists(os.getcwd()+"/ChromeData"):
        shutil.rmtree(os.getcwd()+"/ChromeData")
    os.makedirs(os.getcwd()+"/ChromeData")#directorio objetivo
```

Figura 5.3: Verificación y creación del directorio objetivo.

5.4.2 Recolección

Una vez detectado y generado el directorio de almacenamiento en la unidad extraíble, se procede a la copia de los artefactos en dicho directorio, esta actividad se debe realizar sin emplear ninguna tarea de escritura; esto para evitar cualquier tipo de alteración de la información recolectada.

En la Figura 5.4, se puede apreciar la función de Python que permite cargar los artefactos correspondientes al historial en el directorio objetivo. Se ha seguido un proceso similar para la carga de los diferentes artefactos.

```
#Las cookies
try:
    shutil.copy(os.path.join(pathChrome+"/Cookies"),os.getcwd()+"/ChromeData/Cookies")
```

Figura 5.4: Recolección de las cookies de Google Chrome.

5.4.3 Preservación

Una vez que los artefactos web son recolectados en el directorio creado que contiene el volumen extraíble, se asigna el método de preservación basado en valores hash. Esta asignación se realiza empleando la librería de Python "hashlib".

La función para asignar valores hash es llamada desde la ejecución del programa principal una vez que cada artefacto es almacenado; luego cada valor hash generado es almacenado en un fichero. En la Figura 5.5, se muestra los archivos generados por la herramienta. En la Figura 5.6 se muestran los artefactos recuperados para el navegador Firefox Mozilla; además en la Figura 5.7, se muestra el archivo resultante para los artefactos almacenados de Firefox Mozilla.

ChromeData	24/7/2018 19:00	File folder	
FirefoxData	20/7/2018 15:02	File folder	
HashValuesCrhome.txt	20/7/2018 15:00	Text Document	1 KB
HashValuesFirefox.txt	20/7/2018 15:02	Text Document	1 KB

Figura 5.5: Archivos generados por la herramienta.

cache2	27/6/2018 20:59	File folder	
CacheFireFoxApps	27/6/2018 19:16	File folder	
OfflineCache	26/6/2018 0:59	File folder	
safebrowsing	27/6/2018 20:59	File folder	
startupCache	27/6/2018 20:59	File folder	
cookies.sqlite	20/7/2018 15:00	SQLITE File	512 KB
formhistory.sqlite	20/7/2018 15:00	SQLITE File	192 KB

Figura 5.6: Artefactos de Firefox Mozilla recolectados.

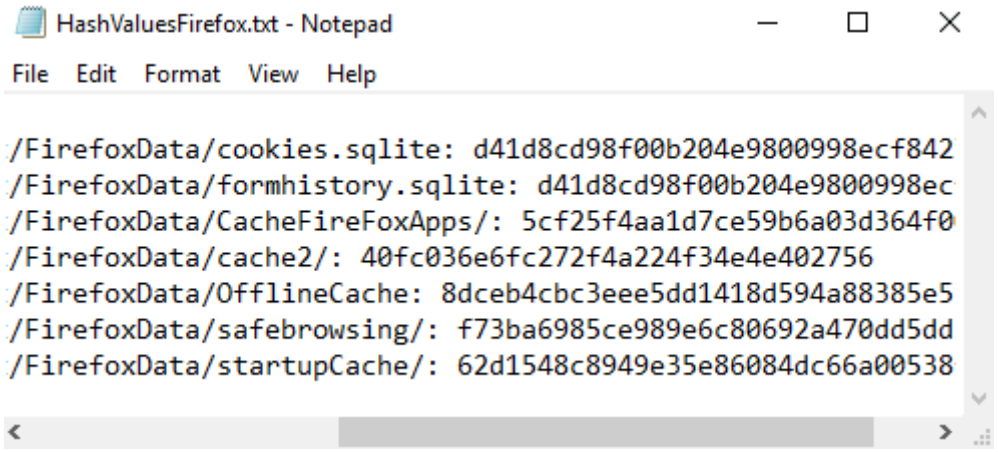


Figura 5.7: Fichero resultante de los artefactos de Firefox.

5.5 Discusión y Conclusiones de la Herramienta

Se ha desarrollado una herramienta de automatización dirigida a la fase de recolección y preservación de la evidencia web, esta permite al investigador forense extraer artefactos web específicos de dos de las aplicaciones más empleadas (Google Chrome y Firefox Mozilla) por los usuarios, para interactuar con aplicaciones en la web a la vez que extrae las funciones hash de la información recolectada para garantizar su posterior integridad.

Si bien, en las pruebas iniciales se aprecia una mejoría en los tiempos de las fases de recolección y preservación, la aplicación es muy específica; dado que puede requerirse la adquisición de artefactos originados en otras aplicaciones. Por lo que, dado a la simplicidad del desarrollo experimentado, es factible el elaborar herramientas que optimicen los procesos de peritaje propios del investigador.

También se ha determinado que es posible optimizar la herramienta aplicando conceptos de paralelización, pues es posible que mientras se realiza la fase de preservación de los artefactos procedentes de una aplicación, los artefactos de una segunda aplicación pueden ser recolectados. Esto con el objetivo de que el investigador forense pueda optimizar el tiempo a la vez que realiza un peritaje basado en buenas prácticas.

6. Prueba de Conceptos

En este apartado se diseñará y planteará una evaluación de la factibilidad de la aplicación de la metodología propuesta a través de una prueba de concepto y se verificará que información es recolectada y generada durante el mismo. Para proceder a la validación de la metodología se ha propuesto un escenario real en el contexto de la educación superior en la Universidad de Cuenca dentro de la facultad de Ingeniería. En el siguiente apartado se presentan los detalles del escenario propuesto.

6.1 Escenario

Como se mencionó, el escenario propuesto está basado en una situación propia y lamentable en el ámbito universitario. Es un caso supuesto, pero que muchas veces resulta complejo dentro de este dominio. El contexto específico en el que se desarrolla el escenario propuesto es una prueba realizada a los estudiantes de tercer nivel de la Facultad de Ingeniería en la asignatura de Probabilidad; en la cual el docente ha decidido hacer uso del centro de cómputo, para que los estudiantes puedan utilizar la plataforma virtual de aprendizaje (Evirtual) para rendir una evaluación y registrar sus respuestas, en el horario de 13h00 ha 15h00 el 3 de Julio del 2018. El desarrollo de esta actividad se muestra Figura 6.1

Esta prueba de concepto fue seleccionada como una prueba de laboratorio en espacios académicos, dada la factibilidad de su ejecución. Ésta no constituye un problema común dentro de la Universidad, puesto que, al ser los reglamentos y las normas claras, los estudiantes evitan este tipo de situaciones. Sin embargo, se ha elegido este dominio por cuanto reúne características que pueden constituir un ejemplo claro para el uso de la metodología planteada en este trabajo de titulación. Siendo únicamente con fines ilustrativos.

La evaluación de conocimientos de la asignatura se desarrolla con normalidad; hasta que, en un momento dado, el docente sospecha de un posible caso de copia por parte de uno de los estudiantes, pues afirma a ver visto en la pantalla del estudiante, que éste hacia uso de un sitio web diferente a la plataforma permitida, por lo que el docente procede a retirar el examen y pedirle al estudiante que se retire dejando todo en el estado actual.

Por su parte el estudiante, ante el cuestionamiento del docente, manifiesta que no se encontraba en ninguna otra aplicación simplemente abrió una nueva pestaña en el navegador por error. Este cierra todas las aplicaciones que se encontraban en funcionamiento, retirándose y dejando el ordenador encendido.

El docente ha solicitado al investigador verificar qué actividades realizó el estudiante en su máquina en el periodo de tiempo de las 13:00 y el momento que el estudiante se retira 14:50.

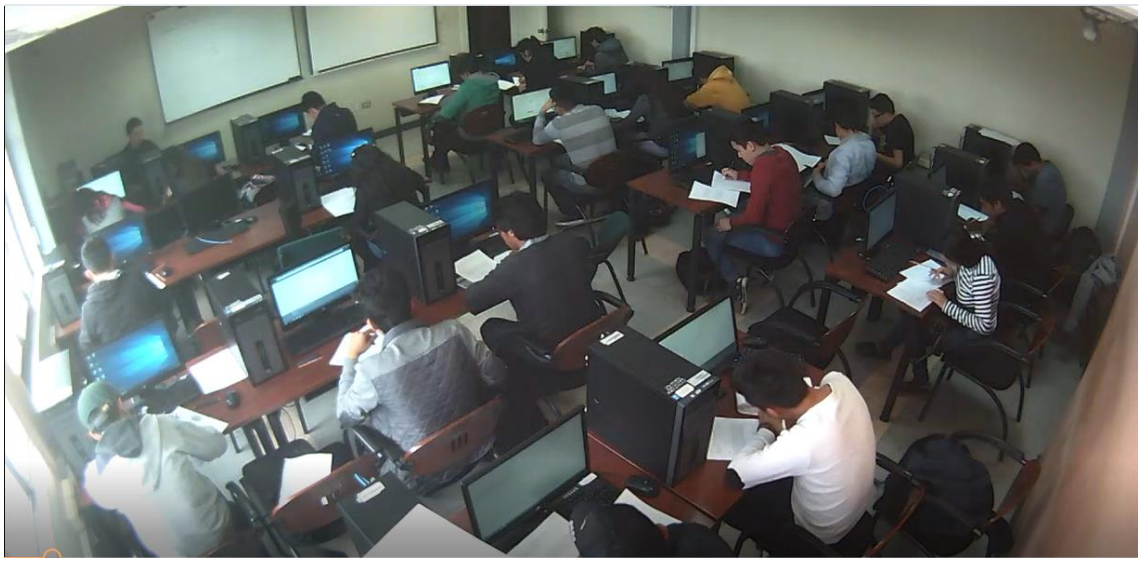


Figura 6.1: Ambiente en el que se desarrolla la prueba de Probabilidad.

6.2 Aplicación de la Metodología

En este apartado se describe detalladamente como la metodología ha sido aplicada al caso mencionado, considerando cada una de las actividades enumeradas y descritas en el apartado anterior.

6.2.1 Identificación de Evidencia Web

Entrada: La entrada para esta etapa es el ordenador donde el estudiante realizaba el examen.

Se procede a identificar al ordenador con un código único para identificar la evidencia proveniente del mismo.

Código del ordenador: C001.

Adicional al código de identificación en el contexto de la investigación, se verifica el identificador físico único del dispositivo en este caso particular el número de serie del CPU, como se puede apreciar en la Figura 6.2.

Número de serie del ordenador: MXL41213Y0

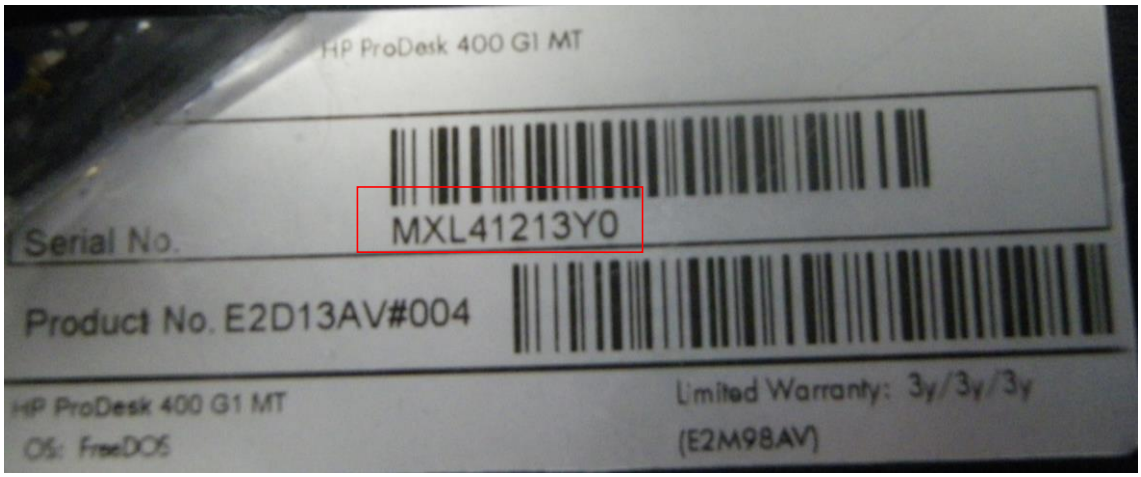


Figura 6.2: Número de serie del ordenador objeto de la investigación.

Luego se desconecta el equipo de la red de acuerdo con lo recomendado previo al inicio de las actividades de investigación como se puede apreciar en la Figura 6.3.

Figura 6.3: Periféricos de red desconectados.

Una vez asegurado que no exista acceso remoto al equipo se procede con las actividades concernientes a esta fase señaladas en la metodología, las mismas que se muestran en la Figura 6.4.

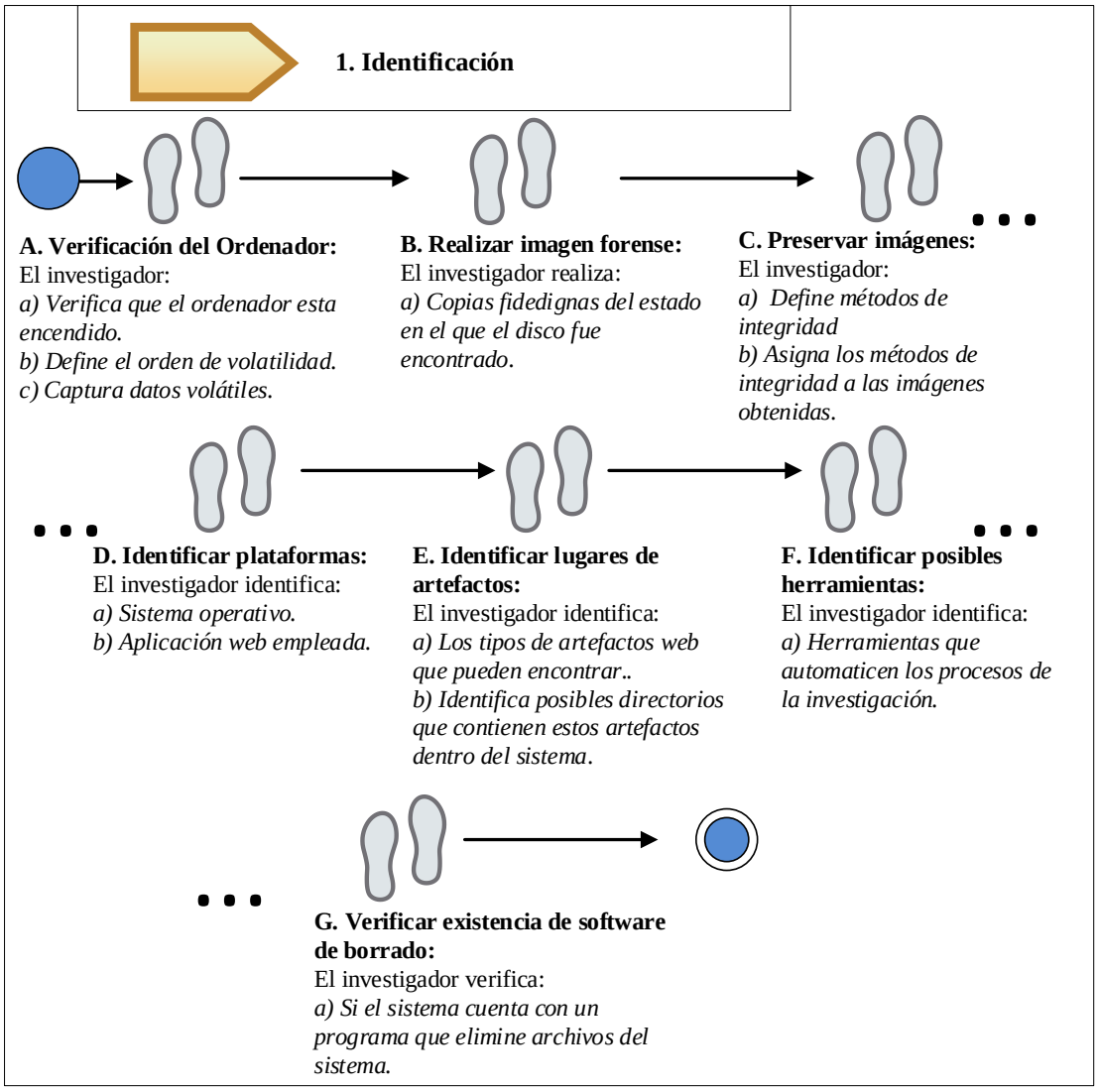


Figura 6.4: Actividades de la fase de Identificación.

A. Verificar el estado del ordenador

El ordenador C001, se encuentra encendido como se aprecia en la Figura 6.5, y no se evidencia la existencia de procesos de borrado de información ejecutándose. Al estar encendido siguiendo la presente guía se procede a analizar la volatilidad de la evidencia.

Figura 6.5: Estado en el que el ordenador C001 fue encontrado.

Analizar la volatilidad de la evidencia

De acuerdo con las recomendaciones antes mencionadas, en la presente actividad se recolecta la información donde puede existir evidencia proveniente de sitios web en el siguiente orden de volatilidad: 1) Memoria física, 2) Archivos temporales y 3) Disco.

Luego de establecer el nivel de prioridad, la información es recolectada utilizando el software OS Forensics; luego, para garantizar su integridad se extrae el valor de la función hash, como se indica en la Figura 6.6. La captura de la memoria ha sido almacenada con el identificador “RAM_Equipo001”.

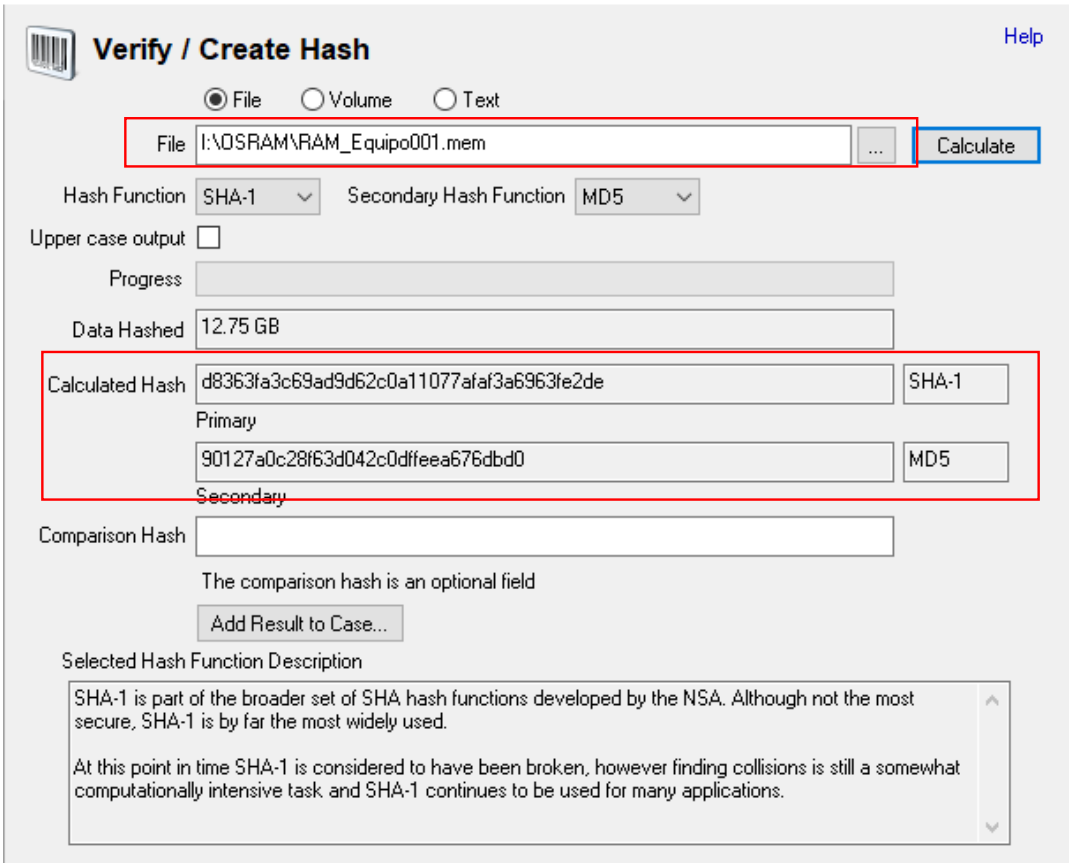


Figura 6.6: Captura de las funciones hash de la captura de memoria RAM.

B. Realizar las imágenes forenses

La imagen generada del disco del ordenador C001, fue realizada con OS Forensics, habilitando el bloqueo de escritura; de forma que la información se mantenga íntegra, como se aprecia en la Figura 6.7. La imagen del disco es generada en formato Virtual Hard Disk (.vhd).

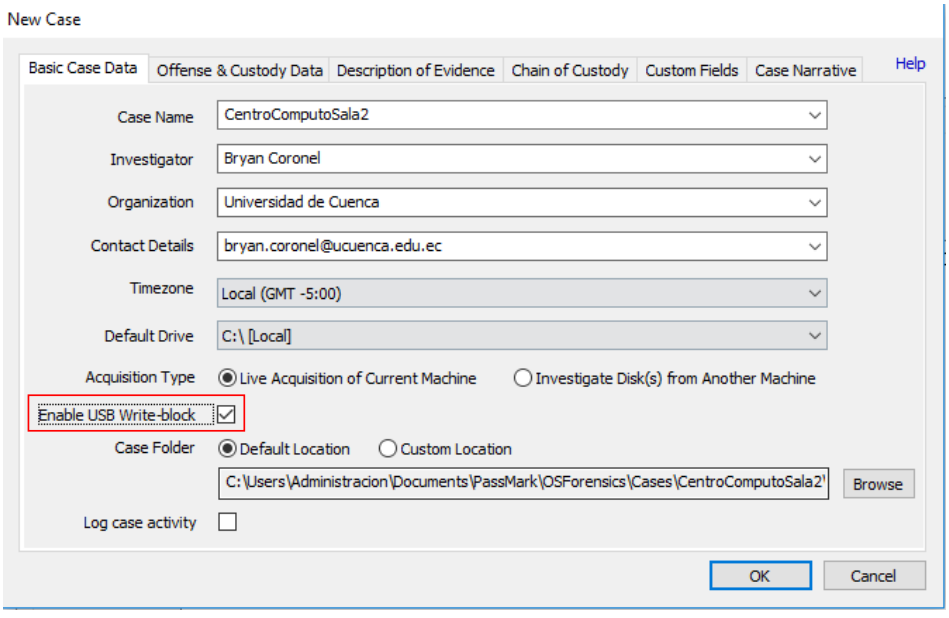


Figura 6.7: Creación del caso de investigación bloqueando la escritura sobre el disco.

C. Preservar imágenes forenses

Al momento que la imagen del disco es generada, se procede a extraer los valores hash y comprobar la integridad de la evidencia siempre que se necesite. El valor hash de la imagen del disco puede ser apreciada en la Figura 6.8. La imagen del disco ha sido identificada como “ImagenEquipoUsuario001”.

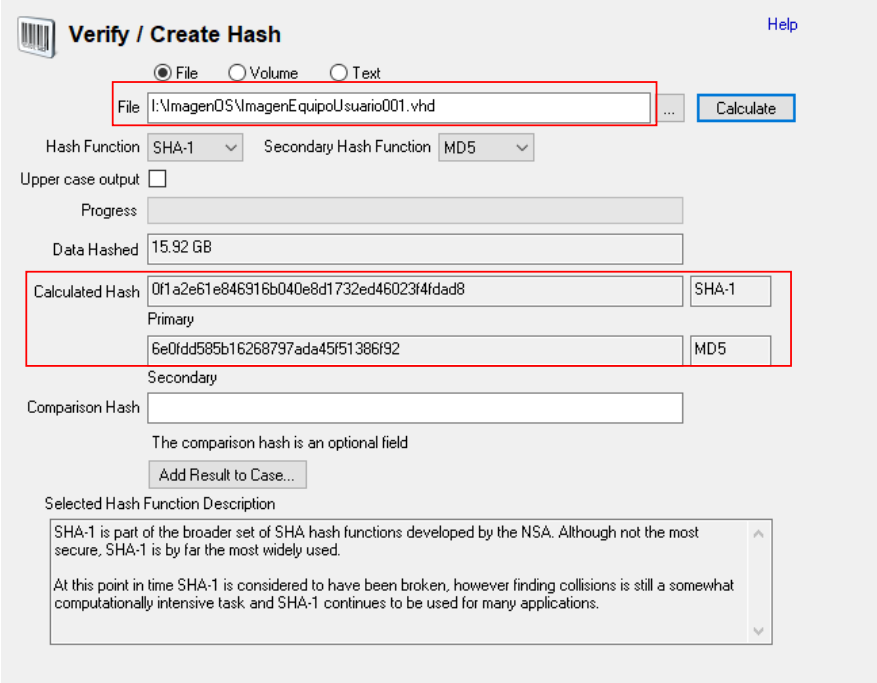


Figura 6.8: Valores Hash de la imagen ImagenEquipoUsuario001.

Adicionalmente, siguiendo las guías de preservación, se han realizado respaldos de la evidencia adquirida en esta fase.

D. Identificar las plataformas relacionadas

Sistema operativo identificado como Windows 10.

Navegadores web instalados en el centro de cómputo: Google Chrome, Firefox Mozilla y Edge.

E. Identificar los posibles lugares donde puede estar la evidencia web

Se puede encontrar evidencia web de la aplicación en:

- Historiales de navegación (Archivos de los navegadores).
- Cachés de navegadores (Para el caso de Windows, en la carpeta AppData).
- Cookies que almacenan los sitios web en el ordenador.
- Rastros de evidencia en memoria volátil.

- Elementos descargados
- Logs del sistema

Google Chrome almacena sus datos de navegación (cachés, cookies, historiales, etc) en el directorio:

C:\Users\[usuario]\AppData\Local\Google\Chrome\User Data\Default

También se identificó que Google Chrome almacena un fichero con el historial de sus accesos (loggins el término en inglés) en la misma ruta.

Por su parte Mozilla Firefox almacena sus datos de navegación en sus directorios:

Para cookies, e historiales:

C:\Users\[usuario]\AppData\Roaming\Mozilla\Firefox\Profiles\ [secuencia de números y letras].default

Para la caché:

C:\Users\[usuario]\AppData\Local\Mozilla\Firefox\Profiles\ [secuencia de números y letras].default

F. Identificar las herramientas que se pueden emplear

Las herramientas empleadas en esta investigación son el OS Forensics y Autopsy para el análisis; por su compatibilidad con el sistema de archivos NTFS Windows.

G. Identificar si existe software de borrado de archivos

Se examinó los programas instalados dentro del ordenador y no se encontró un software especial para borrado de archivos.

Salidas: Imágenes forenses generadas.

6.2.2 Recolección de Evidencia Web

Entradas: Las imágenes generadas del disco (ImagenEquipoUsuario001) y de la memoria RAM (RAM_Equipo001).

Las actividades recomendadas en la metodología al investigador se muestran en la Figura 6.9.

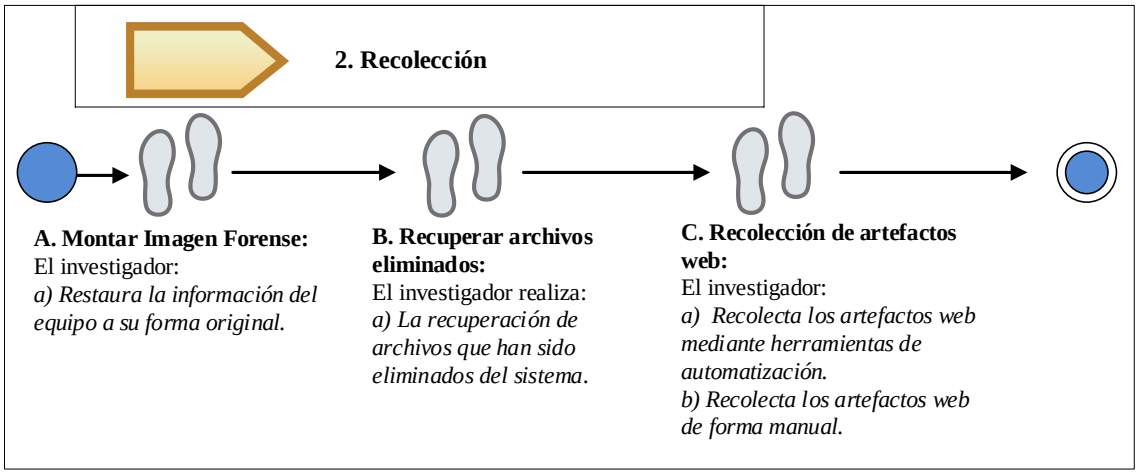


Figura 6.9: Actividades de la fase de Recolección.

A. Montar la imagen

Se verifica que la evidencia esta íntegra; se procede a comparar los valores hash de la evidencia original (Figura 6.8) con el valor hash de la imagen de la cual extraeremos la evidencia que se aprecia en la Figura 6.10; esto para corroborar que el análisis de la evidencia sea fiable.

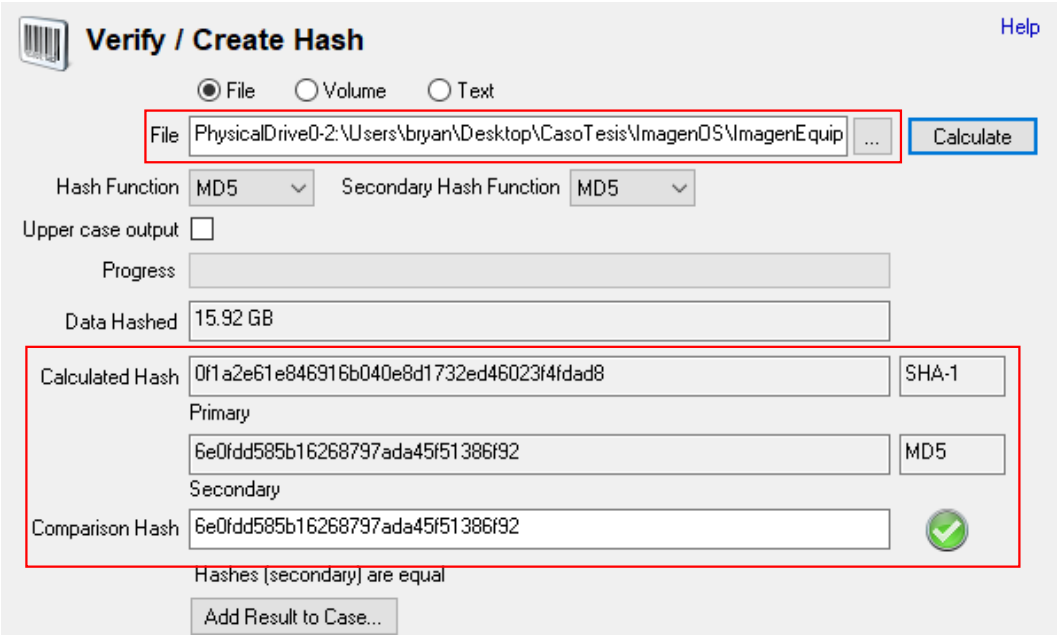


Figura 6.10: Verificación de integridad de la imagen “ImagenEquipoUsuario001”.

Se monta la imagen del disco con ayuda de la herramienta OS Forensic y se permite únicamente la lectura de la información que se va a cargar en este caso particular en la unidad E, como se parecía en la Figura 6.11.

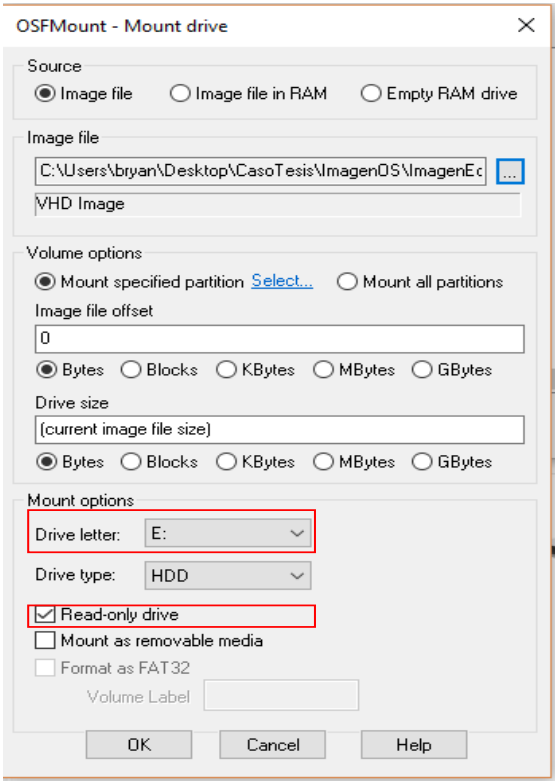


Figura 6.11: Carga de la imagen en la unidad E y se permite únicamente su lectura.

B. Recuperar archivos eliminados

Mediante el software OS Forensics se realizó la búsqueda de archivos eliminados, donde se encontró la existencia de varios archivos eliminados, pero en su gran mayoría pertenecían a archivos temporales empleados por sitios web (como íconos) y archivos con metadata no relevantes a la investigación.

C. Recolectar artefactos web

Se procede a recuperar la evidencia procedente de los sitios previamente identificados como potenciales repositorios de evidencia digital de entornos web.

La fase de recolección ha sido conducida mediante dos métodos, el primero con el uso del software OS Forensics, y el segundo mediante el uso de la herramienta planteada en el apartado 5.

Se recolecta la potencial evidencia para su posterior preservación y análisis. En este caso la información ha sido almacenada como imágenes mediante la herramienta OS Forensics, que permite examinar el disco montado para recolectar la posible evidencia digital de entornos web relevantes para el caso. La evidencia que ha sido considerada es: cachés de navegación, cookies e historiales de navegadores.

La evidencia fue identificada como “ImagenDataWeb001”.

Adicionalmente, se realiza la recolección de los artefactos web, mediante la herramienta planteada para la recolección de artefactos de dos de los navegadores más utilizados como Google Chrome y Firefox Mozilla (Oh et al., 2011). En la Figura 6.12 se muestra el archivo de salida que contiene los artefactos almacenados y su función hash calculada. El script Capturer.py puede ser encontrado en el anexo A.

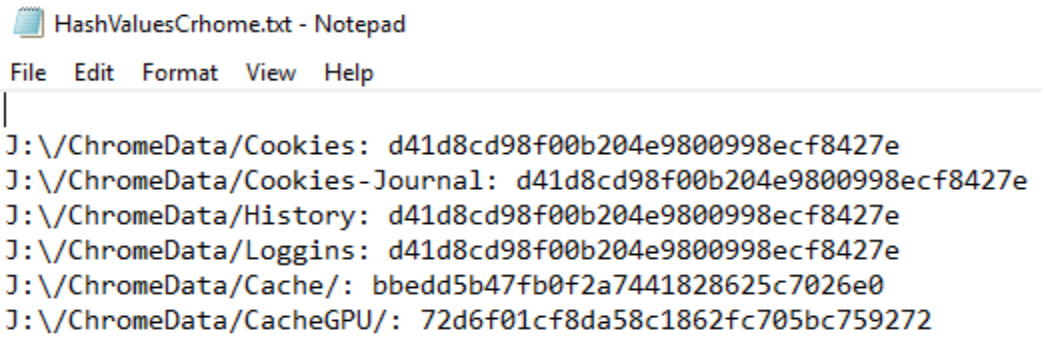


Figura 6.12: Archivo resultante con la ejecución del script Captuer.py para Chrome.

Salida: Datos recolectados (ImagenDataWeb001).

6.2.3 Preservación de Evidencia Web

Entradas: Datos recolectados relevantes a la investigación (ImagenDataWeb001) y los datos volátiles (RAM_Equipo001).

Las actividades recomendadas al investigador para la fase de preservación dentro de la metodología propuesta se muestran en la Figura 6.13.

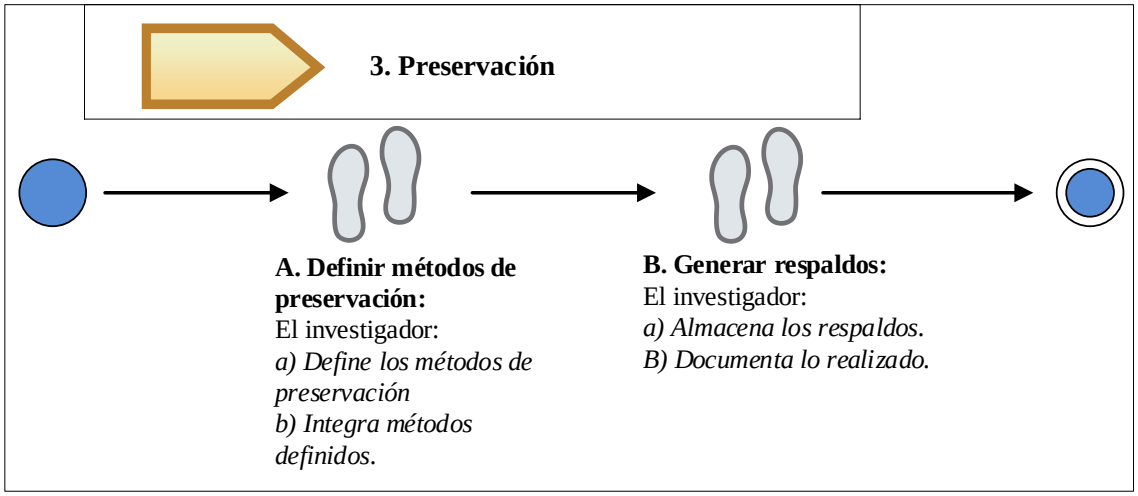


Figura 6.13: Actividades de la fase de Preservación.

A. Definir métodos de preservación

Los métodos de preservación empleados son:

- Extraer valores hash de la evidencia, se sigue el mismo proceso empleado en la imagen del disco y la captura de información volátil.
- Asignar firma digital, se ha utilizado la herramienta OS Forensics; la cual genera un fichero que contiene la firma digital para su posterior comparación. En la Figura 6.14 se aprecia la interfaz de creación de la firma digital provista por OS Forensics.

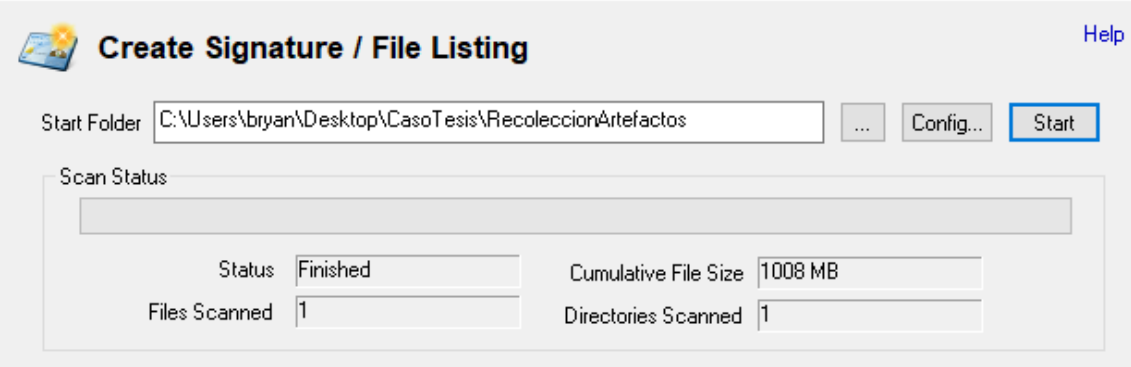


Figura 6.14: Interfaz de creación de firma digital. Fuente: OS Forensics.

B. Generar respaldos

Se han realizado múltiples respaldos de los artefactos recolectados en diferentes locaciones (i.g., disco duro externo y en la nube); almacenando estos bajo el identificador “ExtResp001”. En la Figura 6.15 se muestra el disco duro externo que almacena uno de los dos respaldos realizados junto con los valores hash y la respectiva firma digital.

Figura 6.15: Respaldo físico de la evidencia recolectada

Salidas: Evidencia (ImagenDataWeb001 y RAM_Equipo001). Documentación de métodos de preservación para su posterior verificación y sitio de respaldo.

6.2.4 Análisis de evidencia digital de la web

Entrada: Evidencia preservada (ImagenDataWeb001 y RAM_Equipo001)

Antes de iniciar con las actividades de análisis, se verifica la integridad de la evidencia digital efectuando la verificación de los valores hash, se realiza de la misma verificación de integridad de las imágenes forenses. Por otra parte, la verificación de la firma digital se realiza comparando la firma digital anterior con la de la evidencia que se va a analizar. En la Figura 6.16 se observa la firma que ha sido verificada con éxito y no se registra ningún cambio en la evidencia.

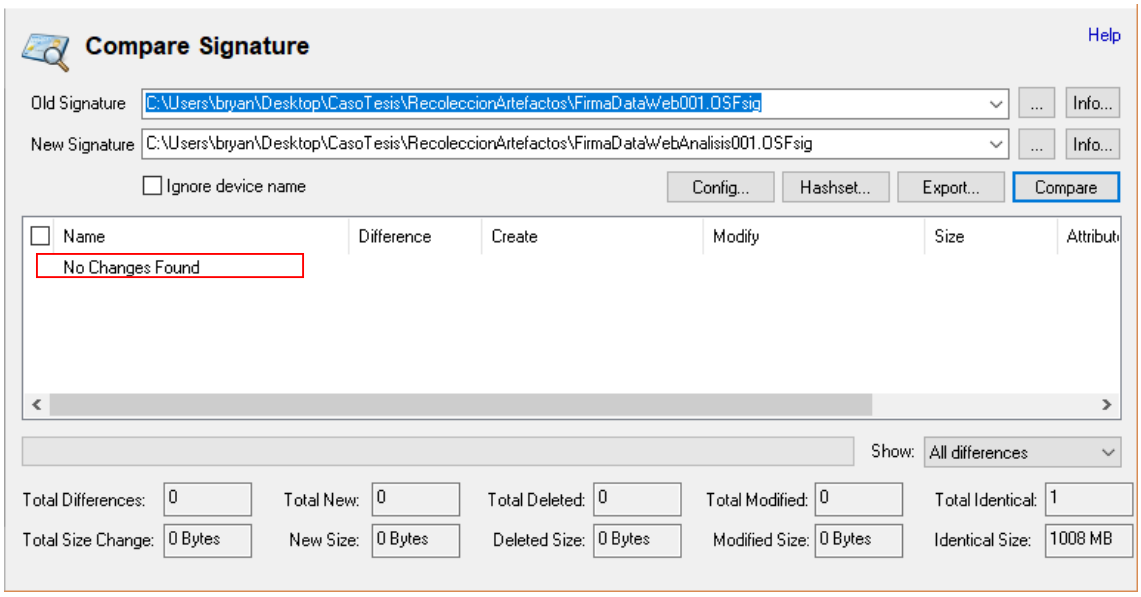


Figura 6.16: Resultado de la verificación de firma digital.

Las actividades recomendadas al investigador para la fase de análisis dentro de la metodología propuesta se muestran en la Figura 6.17.

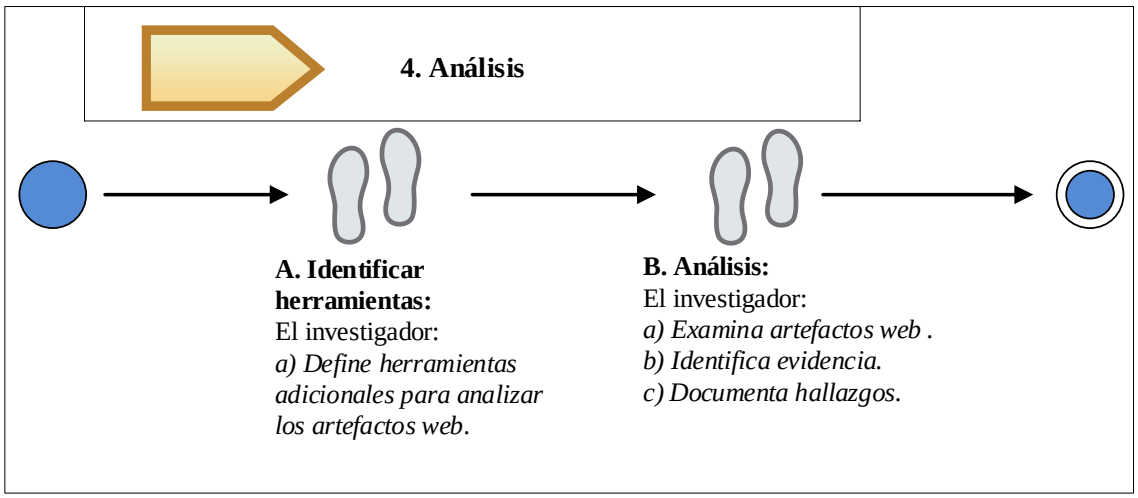


Figura 6.17: Actividades de la fase de Análisis

A. Identificación de herramientas

Las herramientas establecidas en la fase de identificación son ratificadas. Para el análisis de la información recolectada se utiliza el software Autopsy. Pero adicionalmente se emplea el software Belkasoft Evidence Center para el análisis de la información volátil, pues permite una mejor interpretación de la información.

B. Análisis

Para efectuar el análisis, dada la compatibilidad del software Autopsy, es posible utilizar los artefactos web recolectados mediante OS Forensics o mediante la propuesta de herramienta desarrollada en el capítulo 5.

Los artefactos web recolectados son cargados al software Autopsy, esta herramienta facilita la interpretación de los datos relevantes. Una vez que la imagen es cargada en Autopsy, se puede apreciar los datos que la herramienta puede interpretar, como cachés, cookies e historiales de navegación como se puede apreciar en la Figura 6.18.

Cada uno de los artefactos encontrados son examinados, con la ayuda de los metadatos y la herramienta se puede filtrar los artefactos que fueron generados en el periodo de tiempo en el que se desarrollaba la prueba de probabilidad (13:00 a 15:00); pues los metadatos proporcionan la fecha y la hora de la información.

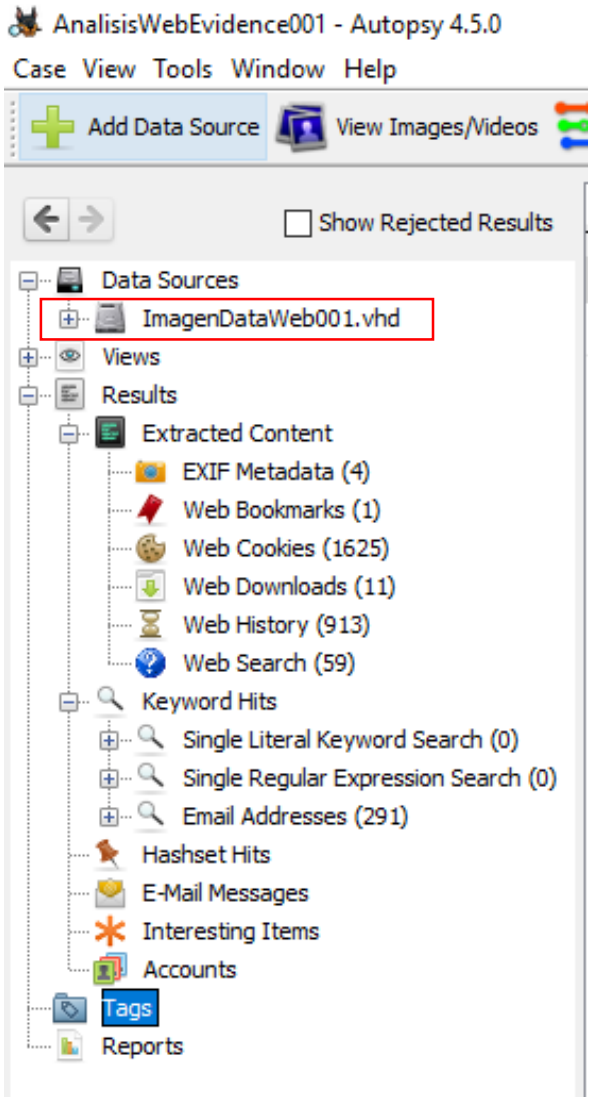
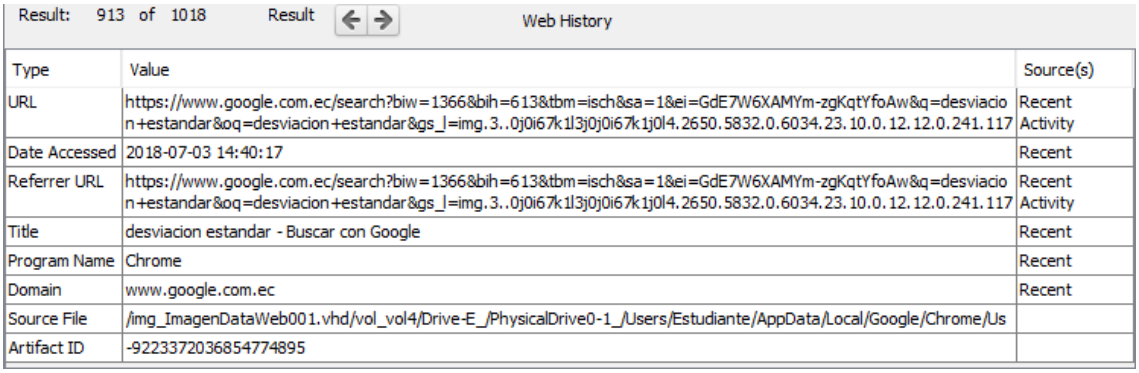


Figura 6.18: Resumen de la información encontrada en la imagen forense cargada.

A continuación, se describe la información relevante que se puede obtener de los diferentes artefactos web como historiales, cachés, cookies y la memoria RAM.

De los historiales, se puede verificar información de los sitios web visitados por el estudiante (i.e., URL completa, fecha y hora, título de la página, dominio y el nombre de la aplicación que se empleó). En la Figura 6.19, se puede apreciar la información de un ítem del historial.

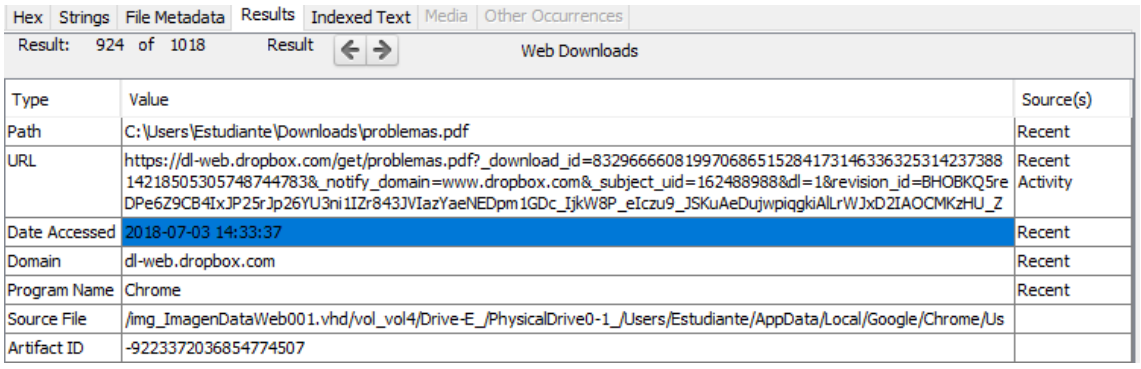


Result: 913 of 1018 Result Web History

Type	Value	Source(s)
URL	https://www.google.com.ec/search?biw=1366&bih=613&tbm=isch&sa=1&ei=GdE7W6XAMYm-zgKqtYfoAw&q=desviacion+estandar&oq=desviacion+estandar&gs_l=img.3..0j0i67k1l3j0j0i67k1j0l4.2650.5832.0.6034.23.10.0.12.12.0.241.117	Recent Activity
Date Accessed	2018-07-03 14:40:17	Recent
Referrer URL	https://www.google.com.ec/search?biw=1366&bih=613&tbm=isch&sa=1&ei=GdE7W6XAMYm-zgKqtYfoAw&q=desviacion+estandar&oq=desviacion+estandar&gs_l=img.3..0j0i67k1l3j0j0i67k1j0l4.2650.5832.0.6034.23.10.0.12.12.0.241.117	Recent Activity
Title	desviacion estandar - Buscar con Google	Recent
Program Name	Chrome	Recent
Domain	www.google.com.ec	Recent
Source File	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/Us	
Artifact ID	-9223372036854774895	

Figura 6.19: Información provista por los ítems del historial.

Historial de descargas, también los navegadores almacenan historiales de descargas; la información que el historial almacena es: URL fuente completa, fecha y hora, dominio, directorio y nombre con que se almaceno el archivo y el nombre de la aplicación que se empleó. En la Figura 6.20 se puede apreciar la información adjunta al ítem del historial de descargas.



Hex Strings File Metadata Results Indexed Text Media Other Occurrences

Result: 924 of 1018 Result Web Downloads

Type	Value	Source(s)
Path	C:\Users\Estudiante\Downloads\problemas.pdf	Recent
URL	https://dl-web.dropbox.com/get/problemas.pdf?_download_id=832966660819970686515284173146336325314237388142185053057487447838_notify_domain=www.dropbox.com&_subject_uid=162488988&dl=1&revision_id=BHOBKQ5reDPe6Z9CB4IxJP25rJp26YU3ni1IZr843JVIazYaeNEDpm1GDc_IjkW8P_eIczu9_JSKuAeDujwpiqgkiAlLrWJxD2IAOCMKzHU_Z	Recent Activity
Date Accessed	2018-07-03 14:33:37	Recent
Domain	dl-web.dropbox.com	Recent
Program Name	Chrome	Recent
Source File	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/Us	
Artifact ID	-9223372036854774507	

Figura 6.20: Información provista por los ítems de descargas.

Cachés: para el análisis de los cachés de navegación, la herramienta empleada permite identificar si los mismos pertenecen a datos de tipo texto, imagen, video o gif. De ser posible también se proporciona una vista previa de los objetos multimedia como se muestra en la Figura 6.21.

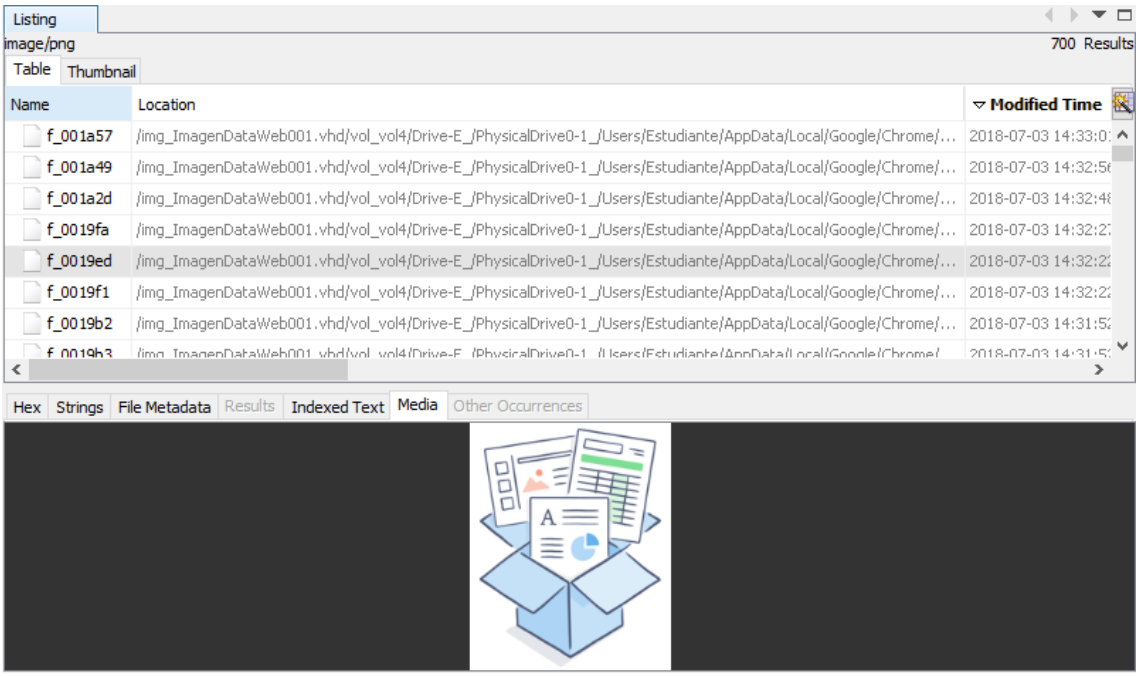


Figura 6.21: Vista previa de un elemento de caché multimedia.

Otro artefacto importante son las cookies dejadas en el ordenador, pues almacenan pequeñas partes de información que podría ser de mucha utilidad en una investigación forense, para el análisis realizado se pudo extraer el inicio de sesión en el periodo de tiempo acorde a la investigación los resultados se abordarán detalladamente en el siguiente capítulo. En la Figura 6.22, se aprecia la información que Autopsy puede extraer para un ítem cookie.

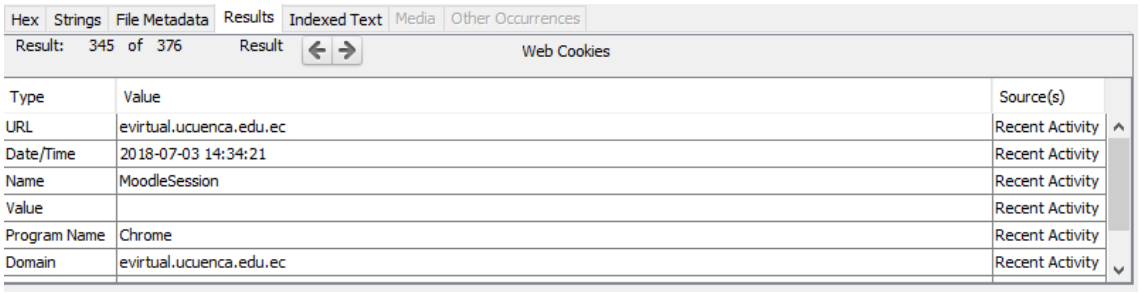


Figura 6.22: Información de un Ítem cookie analizada en Autopsy.

Se continúa con el análisis de los datos volátiles, para lo cual se procede a verificar la función hash de la captura, siguiendo el mismo método que en la imagen del disco como se muestra en la Figura 6.23. Una vez verificado la función hash, se carga la memoria RAM capturada, para lo cual se ha utilizado el software Belkasoft, que permite identificar e interpretar los datos almacenados en la memoria volátil como se aprecia en la Figura 6.24.

Gracias a esta herramienta de interpretación de la memoria RAM, es posible recuperar partes de documentos, imágenes que se encontraban en la memoria

volátil antes de que el ordenador se apagara. En la Figura 6.25, se aprecia una vista de parte de las imágenes recuperadas en memoria RAM del equipo C001.

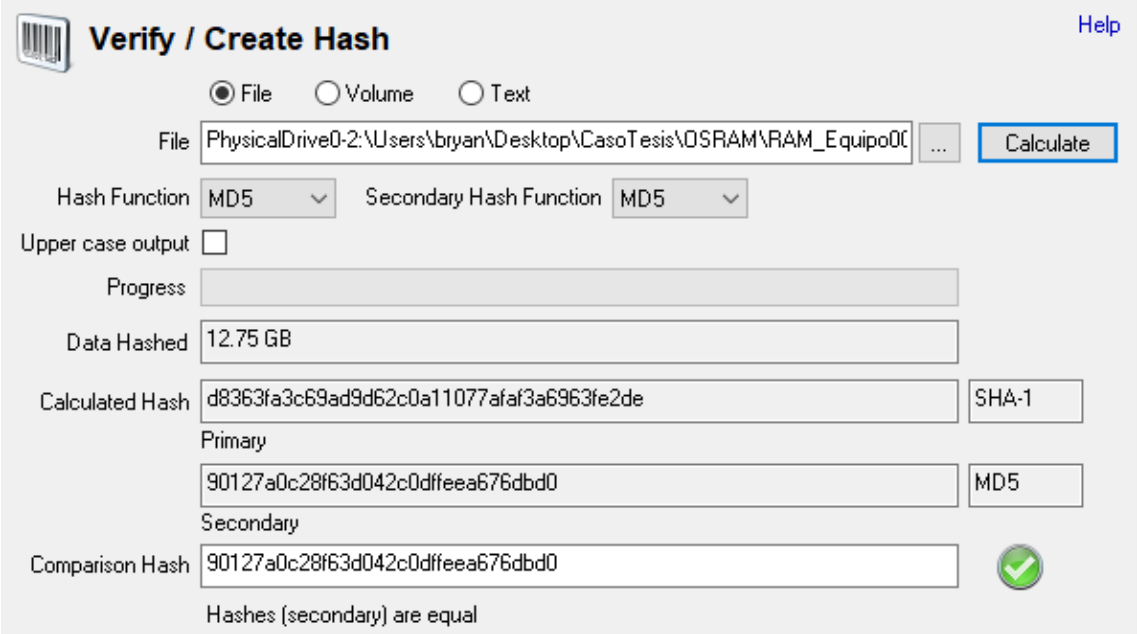


Figura 6.23: Verificación hash del volcado de memoria RAM.

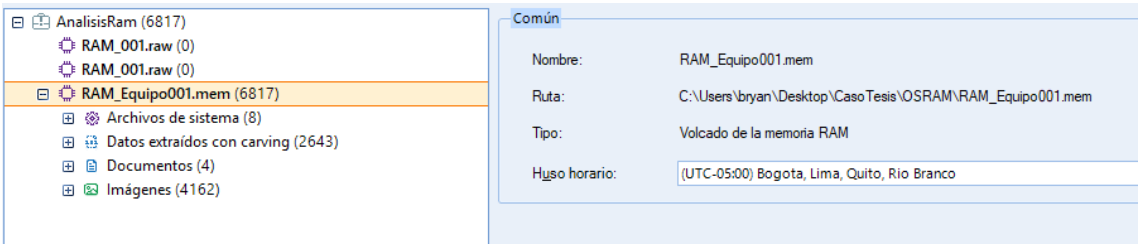


Figura 6.24: Carga de la memoria RAM del equipo C001 en el software intérprete.

Figura 6.25 Partes de Imágenes encontradas en la memoria RAM.

En la siguiente sección se detalla la evidencia encontrada durante la fase de análisis, que constituirá la evidencia digital que sustentará el caso de investigación propuesto.

6.2.5 Presentación de resultados

Las actividades recomendadas al investigador para la fase de presentación dentro de la metodología propuesta se muestran en la Figura 6.26.

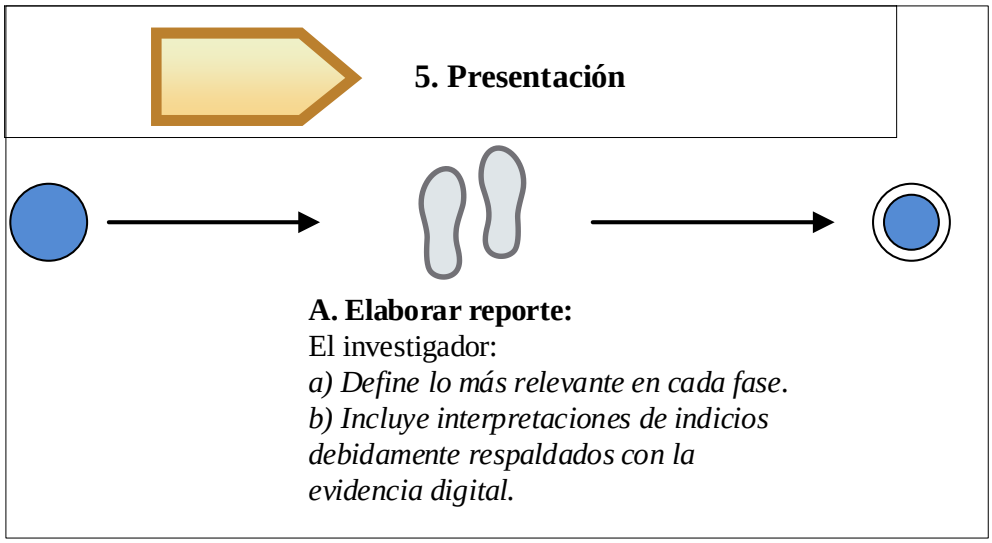


Figura 6.26: Actividades de la fase de Presentación.

A. Elaborar Reporte

En este apartado se detallará la información que ha sido elegida para ser parte del informe de resultados de este caso específico fase por fase.

Identificación

- La identificación única del ordenador objeto de la investigación (código del ordenador y número de serie).
- Los valores hash de la imagen del disco y la captura de la memoria RAM, para una futura posible verificación.

Recolección

- Se describen los elementos que fueron recolectados para proceder al análisis (cachés, cookies e historiales).

Preservación

- Se describe el método empleado al momento de preservar la información recolectada (firma digital).

Análisis

- Se incluye en el informe los análisis que verifican hechos relevantes en el caso de investigación (accesos a sitios web, acciones en sitios web, elementos descargados).

Adicionalmente a la información relevante en cada una de las fases, se ha incorporado al reporte final la información referente al investigador (contactos, profesión). El lector puede encontrar en el Anexo B el informe generado para el caso de investigación planteado siguiendo el formato de informe del consejo de la judicatura.

6.3 Resultados obtenidos

En este apartado se detallan los resultados más importantes respecto a la comparativa entre las herramientas de automatización empleadas en la fase de recolección y la evidencia más relevante encontrada en el análisis de los artefactos web recolectados.

6.3.1 Resultados de recolección

La evidencia digital procedente de entornos web fue recolectada, como se registró en el apartado 6.2.2, pero al momento de proceder con la recolección mediante la herramienta utilizada “OS Forensics”, se observó que, para adquirir la evidencia digital predefinida como procedente de sitios web, el tiempo que consume examinar diferentes directorios es significante; y si se incluye el tiempo que toma asignar un método para garantizar la integridad de la evidencia el tiempo empleado se incrementa. Por este motivo se evaluó la posibilidad de emplear o desarrollar herramientas específicas para adquirir información de forma inmediata. A continuación, se detalla el proceso comparativo empleado.

Se plantea la recolección de los artefactos web más relevantes en el lado del cliente como caché, cookies e historiales (Morioka y Sharbaf, 2016; Oh et al., 2011) de dos de los navegadores más utilizados e instalados en el equipo C001 (Chrome y Firefox). Para efectuar la recolección se emplean las dos herramientas, utilizando el cronómetro del sistema se puede obtener una métrica de tiempo a las dos aplicaciones.

Primero, se empleará OS Forensics para la recolección de la información. Para ello se accede a los directorios de la evidencia y se selecciona los ítems (i.e., cachés, cookies, historiales) que formarán parte de la imagen. El proceso de recolección se puede apreciar en la Figura 6.27. En la que se distingue que el proceso de recolección tuvo una duración de 2 minutos y 9 segundos, mientras que el proceso total, incluyendo actividades en las que interviene el usuario, tiene una duración de 5 minutos y 45 segundos, mismo que incluye localización de directorios y selección de ítems.

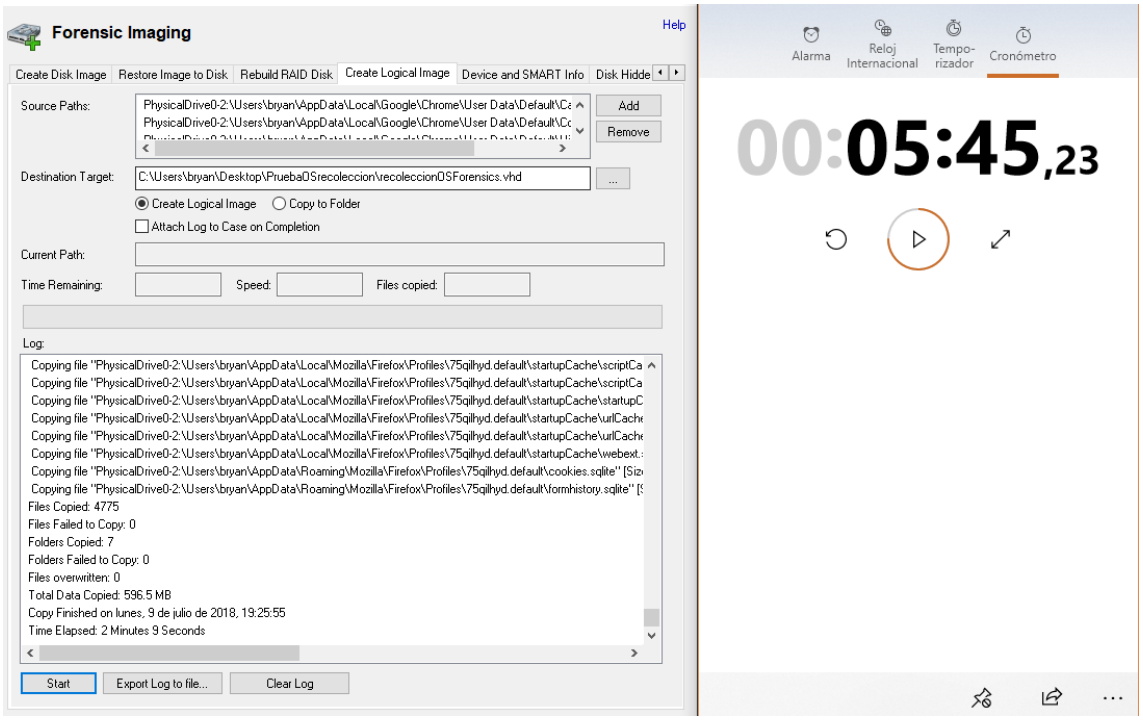


Figura 6.27: Proceso de recolección junto con el tiempo transcurrido.

Una vez que la evidencia ha sido recolectada, ésta debe ser preservada para salvaguardar la integridad de la misma, OS Forensics permite obtener los valores hash de las imágenes extraídas para su posterior verificación. En la Figura 6.28 se aprecia el proceso de extracción de valores hash terminado y el tiempo total que tomó el proceso.

Por otra parte; en la herramienta creada, se incluyó la fase de preservación, lo que permite al investigador recolectar la información relevante para la investigación y garantizar la integridad de la misma, pues se incluye el método de generación de valores hash para garantizar la integridad de la evidencia.

La aplicación inicializa la fase de detección, ésta verifica la existencia del primer navegador y de inmediato empieza a recolectar los artefactos solicitados; simultáneamente extrae los valores hash de los archivos que recolecta como se muestra en la Figura 6.29.

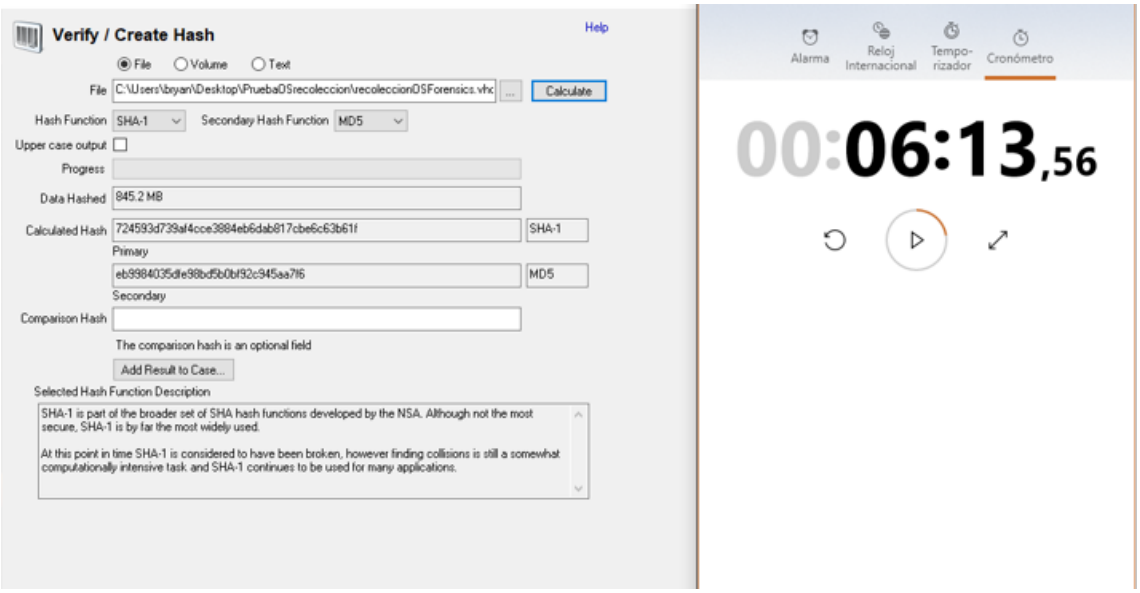


Figura 6.28: Creación de valor hash junto con el tiempo transcurrido.

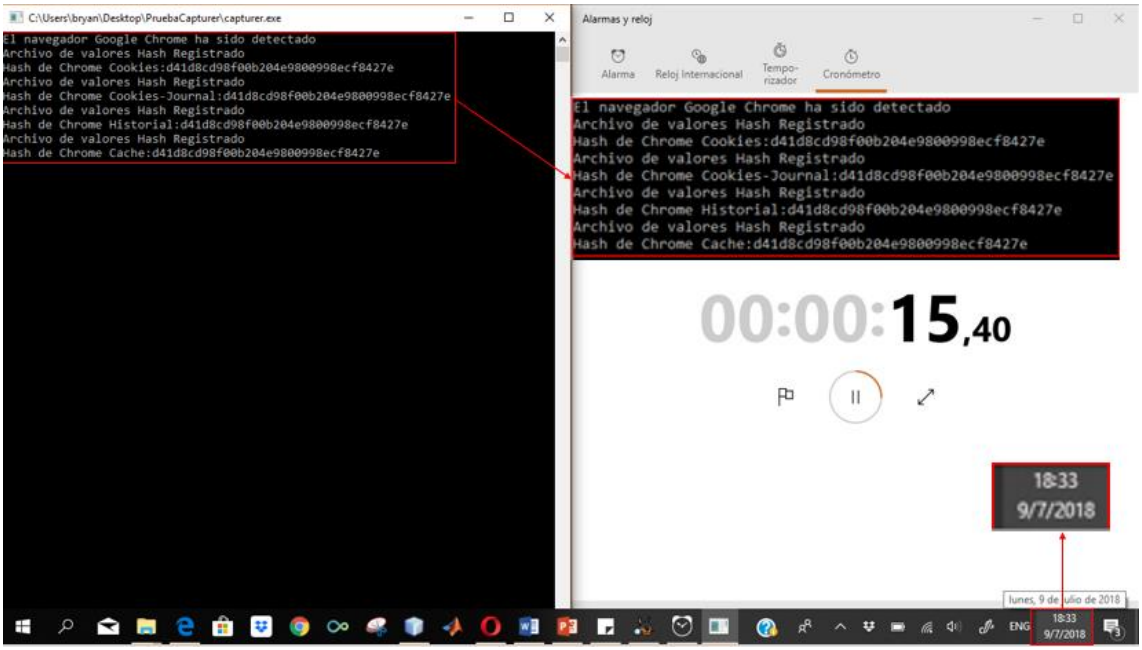


Figura 6.29: Inicio de proceso de recolección y preservación con la herramienta propuesta.

La recolección y preservación de artefactos de Google Chrome termina en 1 minuto y 4 segundos, como se muestra en la Figura 6.30, y de inmediato se prosigue a la recolección de los artefactos del siguiente navegador detectado en este caso Firefox Mozilla, la aplicación inicia de igual manera el proceso de recolección de la información a la vez que la preserva considerando su integridad.

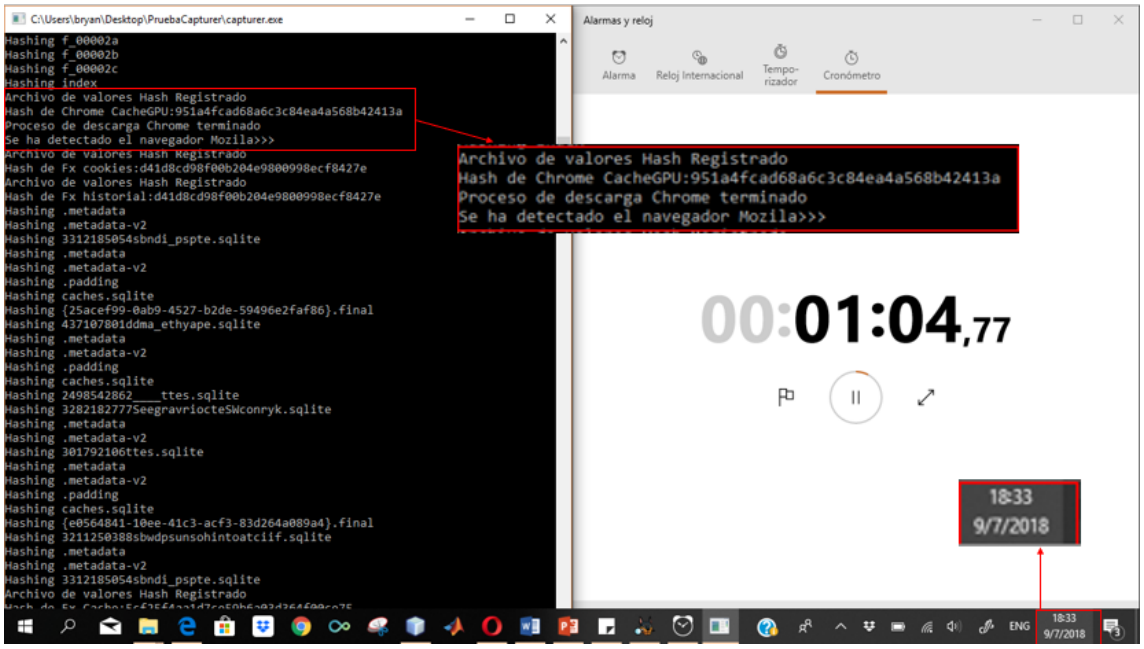


Figura 6.30: Recolección y preservación de artefactos Google Chrome terminado.

Finalmente, el proceso de recolección y preservación finaliza al cabo de 3 minutos y dos segundos, al finalizar el proceso se tiene la información recolectada junto con los ficheros que poseen la información de las funciones hash para cada uno de los artefactos recolectados, como se muestra en la Figura 6.31.

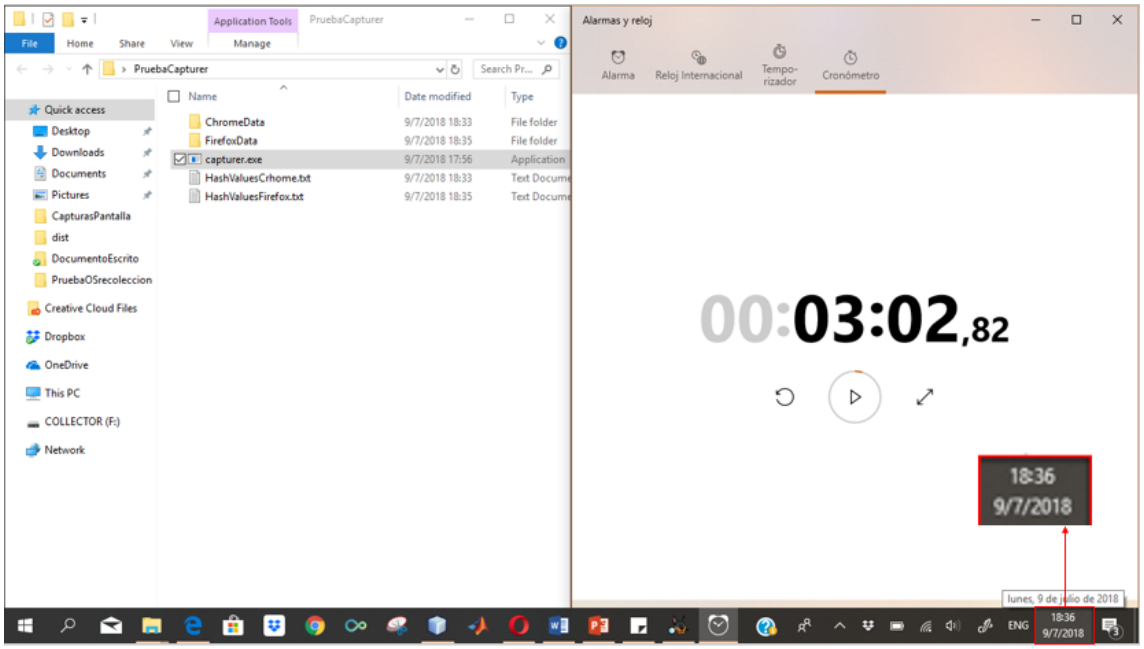


Figura 6.31: Finalización del proceso y ficheros generados.

6.3.2 Resultados del Análisis

En este apartado se presenta lo encontrado en la investigación referente al caso planteado; es decir toda evidencia relevante en este proceso de investigación.

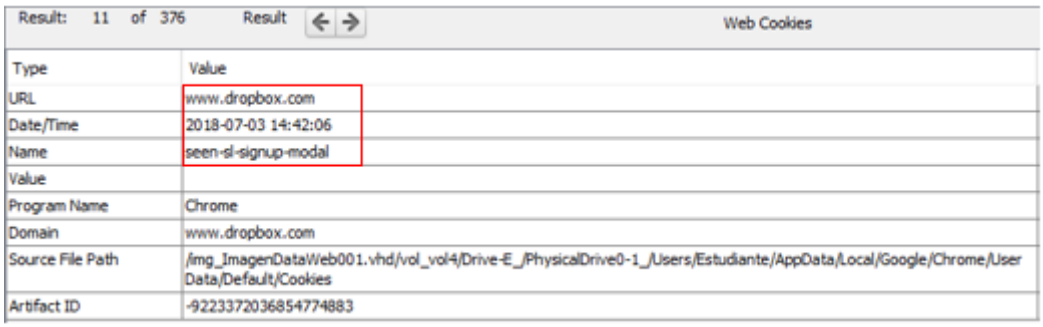
Para ello se ha estructurado de acuerdo a los diferentes tipos de artefactos analizados (cookies, cachés, historiales, etc.). Cabe recalcar que, para analizar los artefactos recolectados, mediante la herramienta propuesta y OS Forensics, dada la compatibilidad de Autopsy no existe distinción en esta fase, pues se recolectaron los mismos artefactos en ambos casos y estos han sido cargados al software de análisis Autopsy.

A. Cookies

En cuanto a cookies, se encontraron un total de 69 cookies, de un total de 1625, en las que su fecha y hora encajan con el desarrollo de la prueba Probabilidad. La evidencia encontrada se muestra a continuación.

En la Figura 6.32 se encontró una cookie de suscripción perteneciente a la aplicación web basada en el modelo SaaS de computación en la nube Dropbox; usado generalmente para almacenamiento de archivos. Esta cookie fue empleada a las 14:42 minutos. Perteneciente al mismo sitio web fue encontrada una cookie para el modo descarga y otra de un rol activo que se muestran en la Figura 6.33 y 6.34 respectivamente. Con estos indicadores se puede determinar que el estudiante pudo realizar actividades de ingreso y descarga en Dropbox.

Adicional a estas cookies que evidencian el uso de la aplicación Dropbox, se ha encontrado cookies procedentes de otros sitios web como Facebook y Google utilizados unos minutos antes que las cookies procedentes como se aprecia en la Figura 6.35. Lo que indica que el estudiante accedió a esta red social y al buscador.



Result: 11 of 376 Result — Web Cookies

Type	Value
URL	www.dropbox.com
Date/Time	2018-07-03 14:42:06
Name	seen-sl-signup-modal
Value	
Program Name	Chrome
Domain	www.dropbox.com
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774883

Figura 6.32: Cookie de suscripción del sitio web Dropbox.

Result: 349 of 376 Result Web Cookies

Type	Value
URL	www.dropbox.com
Date/Time	2018-07-03 14:42:06
Name	seen-sl-download-modal
Value	
Program Name	Chrome
Domain	www.dropbox.com
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774545

Figura 6.33: Cookie para el modo descarga del sitio web Dropbox.

Result: 354 of 376 Result Web Cookies

Type	Value
URL	.dropbox.com
Date/Time	2018-07-03 14:42:06
Name	last_active_role
Value	
Program Name	Chrome
Domain	dropbox.com
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774540

Figura 6.34: Cookie de rol activo del sitio web Dropbox.

Cookies	www.google.com.ec	2018-07-03 14:40:06 COT
Cookies	.facebook.com	2018-07-03 14:40:06 COT

Figura 6.35: Cookies encontrados de Google y Facebook.

Otra cookie de interés es la procedente del Evirtual, lo cual indica que el estudiante obtuvo una sesión en la plataforma universitaria, para realizar la evaluación, la cual se muestra en la Figura 6.36.

Result: 345 of 376 Result Web Cookies

Type	Value
URL	evirtual.ucuenca.edu.ec
Date/Time	2018-07-03 14:34:21
Name	MoodleSession
Value	
Program Name	Chrome
Domain	evirtual.ucuenca.edu.ec
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774549

Figura 6.36: Cookie de sesión procedente del Evirtual.

Comparando la hora de modificación de las cookies, las aplicaciones web accedidas durante la prueba fueron:

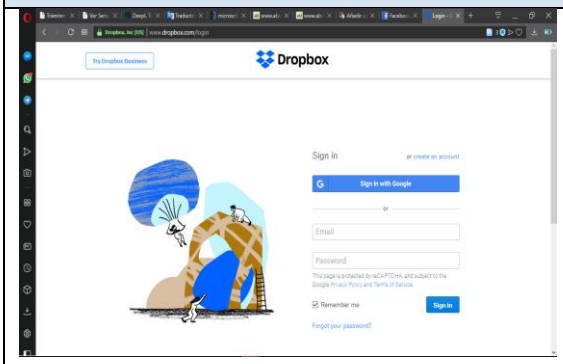
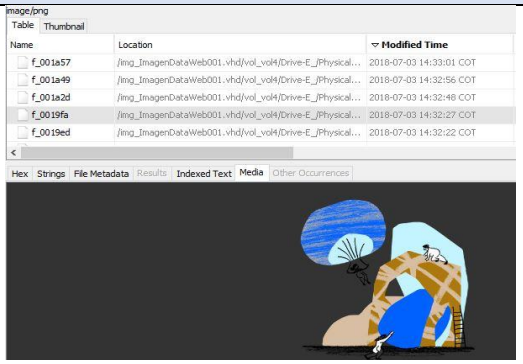
1. Evirtual.
2. Facebook.
3. Buscador de Google.
4. Dropbox.

B. Cachés

El análisis e interpretación de las cachés de navegación encontradas se facilita con el uso de Autopsy, pues permite visualizar los archivos caché en sus diferentes tipos (texto, audio, imagen o video). Con esto se facilita la búsqueda de evidencia relevante para el caso. A continuación, se detalla lo encontrado en las cachés de navegación.

Examinando los archivos de caché identificados como imágenes en formato PNG, se han encontrado imágenes relacionadas a sitios web, en la Tabla 6.1 se puede ver a la imagen en el sitio web y la imagen encontrada durante el análisis de las cachés, cabe recalcar que la fecha de modicación del archivo de caché de la imagen proveniente del caché esta dentro del periodo de tiempo en el que se efectúala investigación.

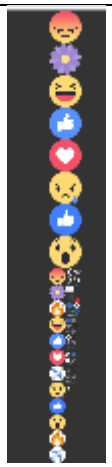
Tabla 6.1: Comparativa de elemento encontrado en el sitio web con el de la caché.

Sitio Web	Elemento Caché
	

Otras imágenes PNG encontradas entre de los archivos de caché, dentro de la fecha y hora de la prueba de Probabilidad, se muestran en la Tabla 6.2.

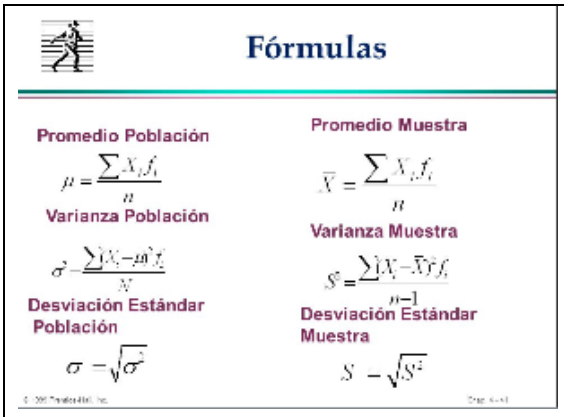
Con las imágenes rescatadas de la caché, se comprueba el acceso a Dropbox y Facebook, pues se evidencian imágenes pertenecientes a estos sitios web modificadas en el horario de investigación. Por otra parte, las imágenes relacionadas con temas probabilísticos no muestran una clara procedencia.

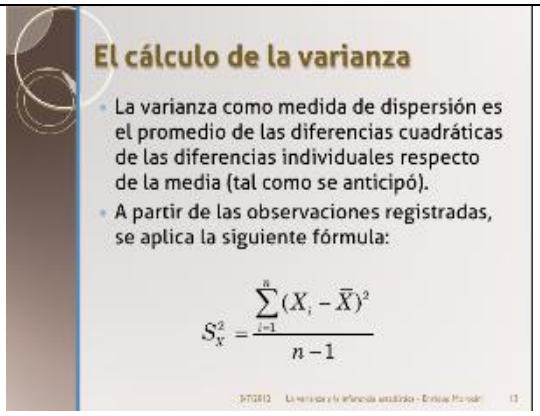
Tabla 6.2: Imágenes de sitios web encontradas en el horario de la prueba.

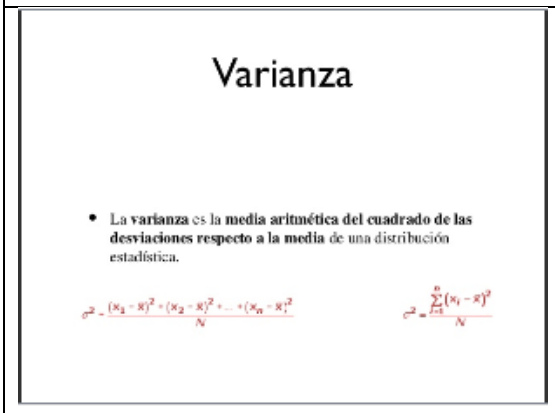
	
	

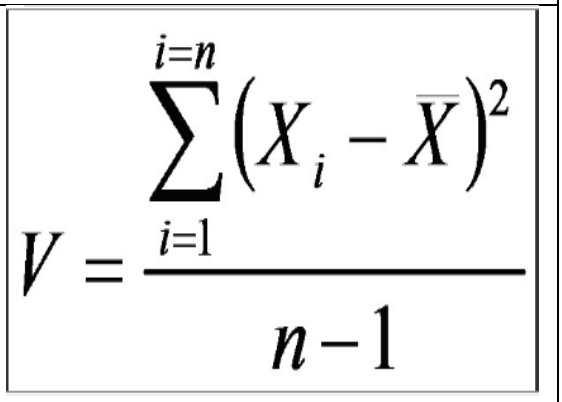
Adicionalmente a estas imágenes, la herramienta también logró identificar imágenes en formato JPEG en el horario de la prueba realizada por los estudiantes. Se lograron identificar imágenes correspondientes a fórmulas matemáticas, teoría de la varianza y otras imágenes de origen desconocido, las imágenes se muestran en la Tabla 6.3.

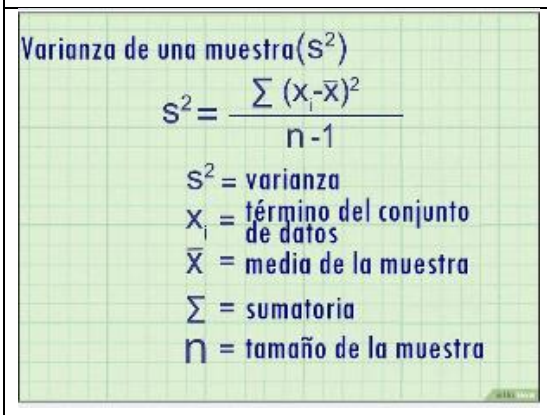
Tabla 6.3: Imágenes JPEG recuperadas de las cachés de navegación.











C. Historiales

Para realizar el análisis de los historiales de navegación, gracias a la herramienta de análisis Autopsy; es posible identificar distintos tipos de historiales como: historiales de búsqueda, navegación, accesos y descargas.

i) Historial de búsqueda

Examinando el historial de búsquedas, se observa que, se realizaron varias búsquedas en Google entre el periodo de tiempo de 14:33:53 hasta 14:40:17; es decir durante el periodo de la prueba realizada. Además, se aprecia las cadenas de texto que fueron ingresadas al buscador; las cadenas de texto encontradas son: “desviación estandar”, “formula varianza” y “probabilidad”. En la Figura 6.37 se muestran los resultados del historial de búsqueda; resaltando el horario objeto de investigación y las diferentes cadenas de texto.

Listing

Web Search

Table | Thumbnail

Source File	Domain	Text	Program Name	Date Accessed	Data Source
History	www.google.com.ec	desviacion estandar	Chrome	2018-07-03 14:40:17 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:40:11 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:10 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:07 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:06 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:02 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:02 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:02 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	probabilidad	Chrome	2018-07-03 14:33:56 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	probabilidad	Chrome	2018-07-03 14:33:53 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	dota 2 leaderboards	Chrome	2018-07-02 18:41:46 COT	ImagenDataWeb001.vhd

Figura 6.37: Resultados del análisis de historial de búsquedas.

ii) Historial de navegación

En análisis del historial de navegación se ha confirmado que el estudiante visitó los sitios web mencionados, y se verificó que las búsquedas dentro de Google fueron efectuadas, pues en la URL se evidencian los parámetros de búsqueda. En la Tabla 6.4, se evidencia la línea de tiempo, con los hechos más relevantes, de acuerdo con el historial de navegación del equipo “C001” extraído mediante Autopsy. A continuación, se detallan estos eventos:

En el evento E1, se registra el acceso al curso virtual “PROBABILIDAD EIET/G1” en la plataforma Evirtual a las 14:31:07.

En el evento E2, se registra un intento de ingreso en la red social Facebook a las 14:31:49.

Seguido del evento E2, en el evento E3 se registra un intento de acceso a la aplicación web Dropbox a las 14:32:27.

Por su parte en el evento E4, se registra la visita de un perfil de Facebook cuyo nombre es “Bryan Coronel” a las 14:32:58.

De manera posterior en el evento E5, se verifica que el estudiante accedió a la prueba colocada en la plataforma virtual a las 14:34:21.

En el evento E6, se registra la finalización de sesión en la aplicación web Dropbox a las 14:40:06.

Finalmente, en el evento E7, se verifica la existencia de búsquedas en Google a las 14:40:11.

Tabla 6.4: Eventos relevantes del historial de navegación procedente de Autopsy

ID	Fecha	URL	Título
E1	2018-07-03 14:31:07	https://evirtual.ucuenca.edu.ec/course/view.php?id=7029	Course: PROBABILIDAD EIET /G1
E2	2018-07-03 14:31:49	https://www.facebook.com/login.php?login_attempt=1ylwv=111	Facebook
E3	2018-07-03 14:32:27	https://www.dropbox.com/login?cont=https%3A%2F%2Fwww.dropbox.com%2Fsh%2Fjz9a5cvemy3q02i%2FAACZLbTCQI37oRY8CERqz26Ga%3Fdl%3D0	Inicia sesión - Dropbox
E4	2018-07-03 14:32:58	https://www.facebook.com/CoR0TApiA	Bryan Coronel
E5	2018-07-03 14:34:21	https://evirtual.ucuenca.edu.ec/mod/quiz/attempt.php?attempt=16347	Prueba Capítulos 5y6
E6	2018-07-03 14:40:06	https://www.dropbox.com/login?src=logout	Login - Dropbox
E7	2018-07-03 14:40:11	https://www.google.com.ec/search?q=formula+varianzaysource=lnmsytbm=ischysa=Xyved=0ahUKEwjI7Iav1oPcAhUoqlkKHbkPC8EQ_AUICigBybiw=1366ybih=613	formula varianza - Buscar con Google

iii) Historiales de accesos

El historial de accesos se forma examinando las direcciones de correos electrónicos en cada uno de los archivos recolectados (eg., cachés, historiales, cookies) con la ayuda de Autopsy. El número de correos identificados dentro de los artefactos web recolectados son 291, como se muestra en la Figura 6.38.

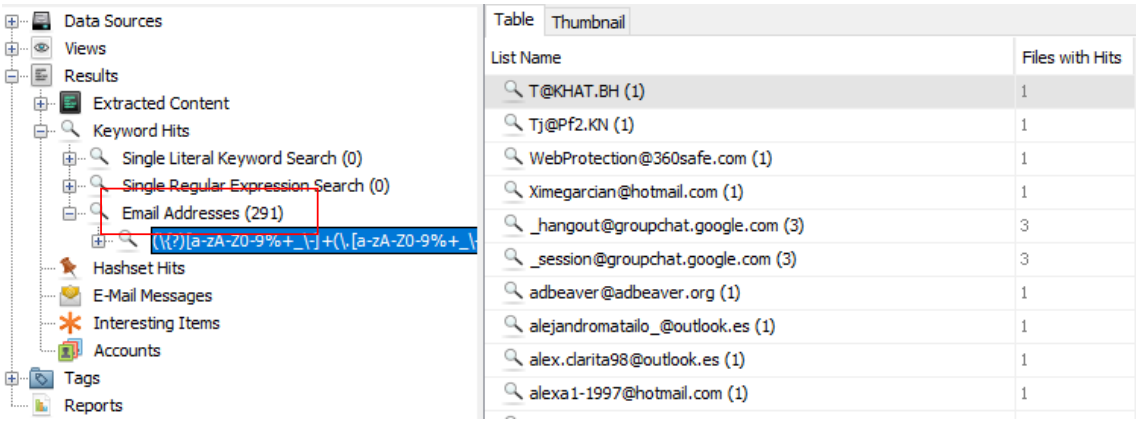


Figura 6.38: Emails identificados por la herramienta Authopsy.

Luego del análisis de las direcciones de correos electrónicos obtenidos, se identificó el acceso a Dropbox con el correo bryantc_hjj@hotmail.com en el horario de la prueba. En la Figura 6.39 se puede apreciar que el último registro corresponde a Dropbox por el correo mencionado; además, se muestra que este acceso fue registrado al mismo tiempo que se desarrollaba la prueba.

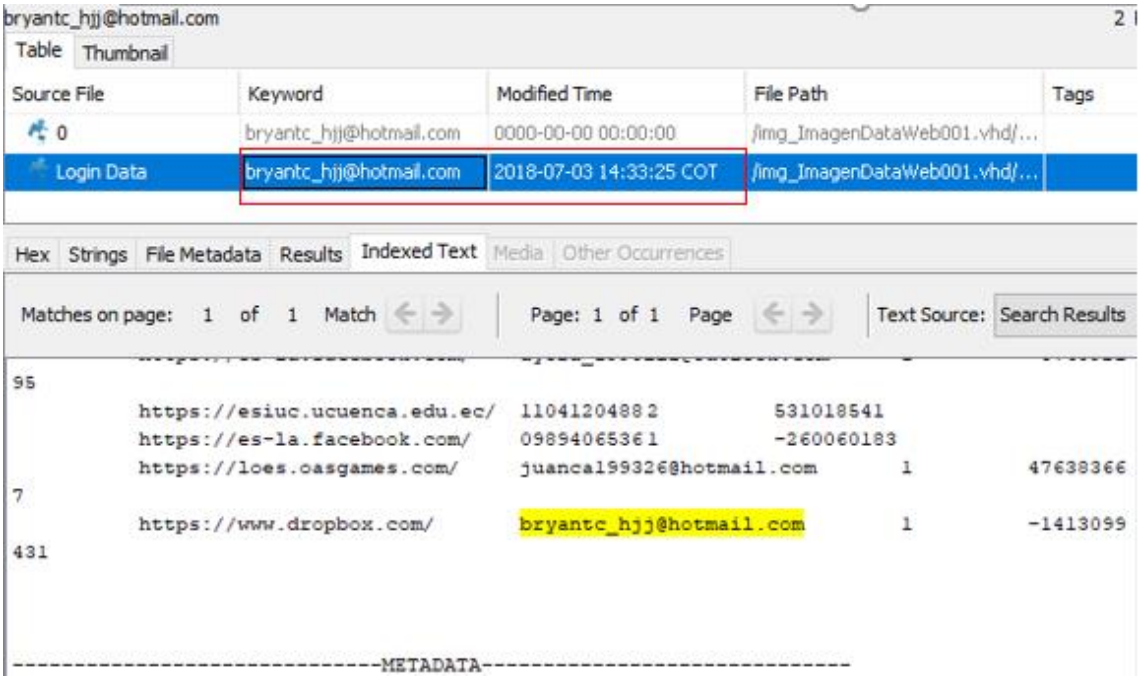


Figura 6.39: Identificación de acceso del correo bryantc_hjj@hotmail.com.

De la misma forma, el correo fue identificado con una sesión activa de Facebook dentro del horario objeto de investigación, como se muestra en la Figura 6.40.

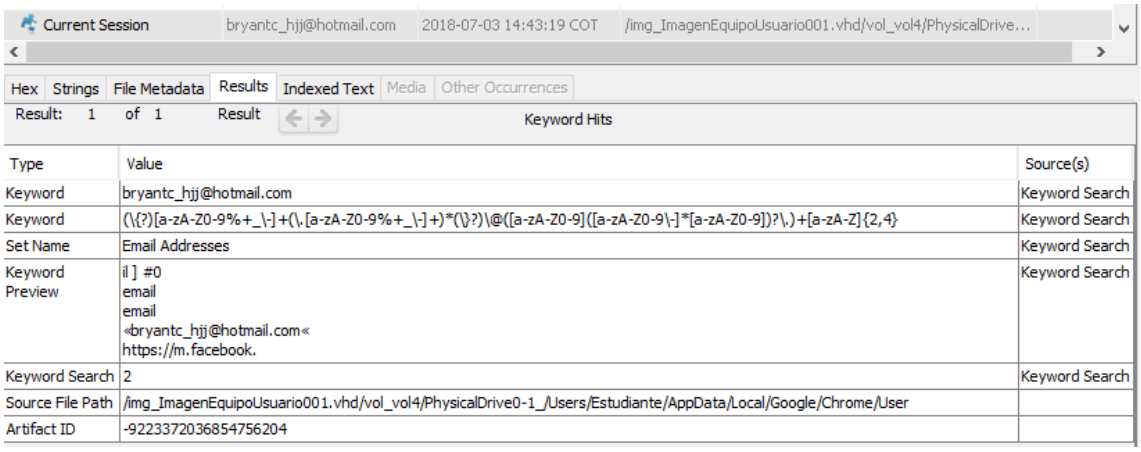


Figura 6.40: Identificación de sesión en Facebook con el correo bryantc_hjj@hotmail.com.

iv) Historial de Descargas

También identificó los archivos que emplean los navegadores para almacenar los metadatos de las descargas. Previo al análisis del historial de descargas se ha examinado el contenido de la carpeta descargas del equipo, empleando la imagen: “ImagenEquipoUsuario001”, la carpeta descargas no posee ningún archivo correspondiente al horario de investigación, como se aprecia en la Figura 6.41.

Se encontró que se han descargado tres archivos en el instante que el estudiante realizaba la prueba. Los tres archivos proceden del sitio web Dropbox, como se muestra en la Figura 6.42.

Adicionalmente se pueden identificar los nombres de los primeros dos ítems:

- Problemas.pdf
- Probabilidad.rtf

Verificando los metadatos de estos archivos, se verifica que los archivos se encontraban en el sistema. La Figura 6.43 muestra los metadatos obtenidos del primero ítem de descargas.

Luego de lo analizado se puede verificar que el estudiante descargó tres archivos Dropbox, luego accedió a los mismos y los eliminó.

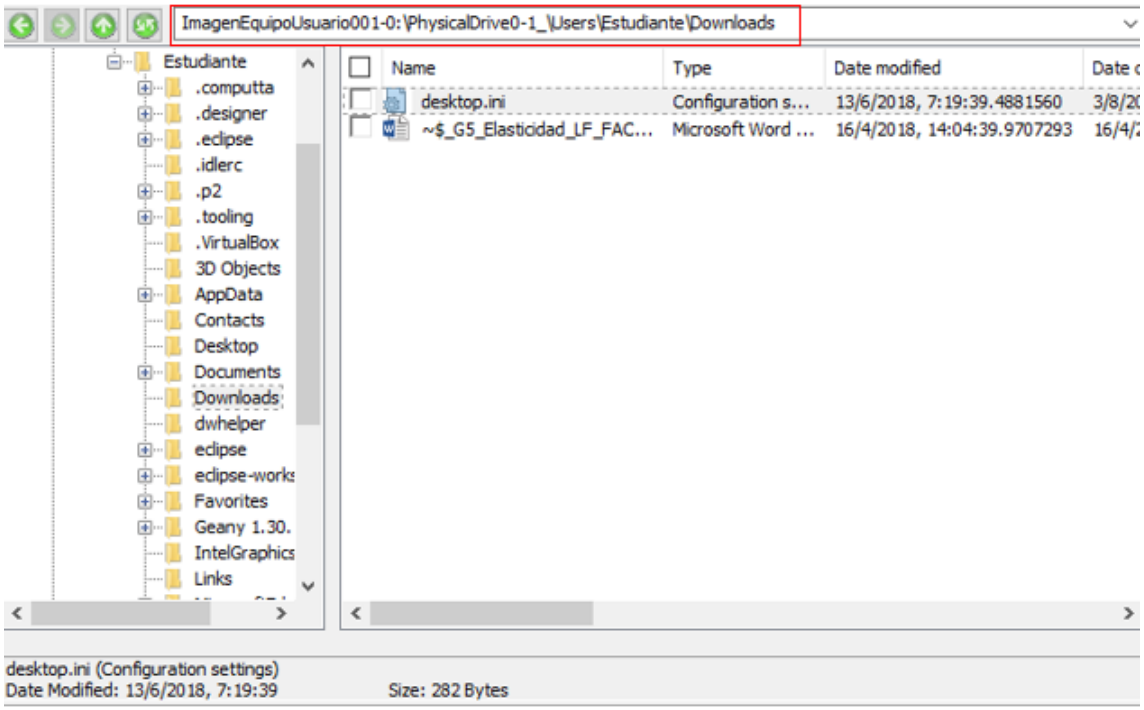


Figura 6.41: Vista del directorio de descargas de la imagen del disco.

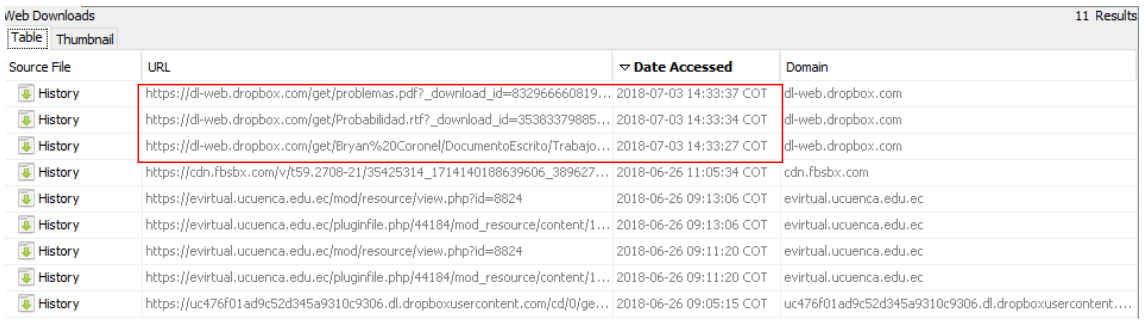


Figura 6.42: Descargas realizadas durante la realización de la prueba.

Type	Value
URL	https://dl-web.dropbox.com/get/Probabilidad.rtf?_download_id=35383379885839616809363210663906418776384178490193600035941201329 4&_notify_domain=www.dropbox.com&_subject_uid=162488988&dl=1&revision_id=BHNn-NcwKHy8ngPgVr_ytHWEjlo-Z2SggIIBPapO2Rgj-tZelM3-26MF7jOWto5nOnTnORJ6eTdH9u-GmsHs2nH4GP8Z-e4Lkp8sfPURLcXldJdKqUptG9bDZdjbISXAHHY&w=AABENdkEmgEbFGnG9eEVeoh0G5OOaR1MI-5a3q5UunckVg
Domain	dl-web.dropbox.com
Program Name	Chrome
Path	C:\Users\Estudiante\Downloads\Probabilidad.rtf
Date Accessed	2018-07-03 14:33:34
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/History
Artifact ID	-9223372036854774508

Figura 6.43: metadatos del primer ítem de descarga.

D. Memoria Volátil

Como se mencionó, el software empleado es “Evidence Center” de Belkasoft, que permite la fácil interpretación de los datos capturados procedentes de la

RAM “RAM_Equipo001”. A continuación, se detallan los datos más relevantes encontrados.

Se verificó que el archivo “Probabilidad.rtf” fue abierto, pues el directorio “*C:/Users/Estudiante/Download/Probabilidad.rtf*” fue visitado como se verifica en la Figura 6.44.

Se verificó la existencia de cinco conversaciones o chats en la memoria volátil, pese a que el texto no es legible, se verificó que dos de las mismas pertenecen a un sitio web desarrollado en PHP como se muestra en la Figura 6.45, cabe recalcar que Facebook esta desarrollado en PHP.

Finalmente se logró identificar información referente a las URLs almacenadas en la captura de RAM, se verificó la existencia de las URLs de: Dropbox, Facebook, Goolge y el Evirtual, como se evidencia en la Figura 6.46.

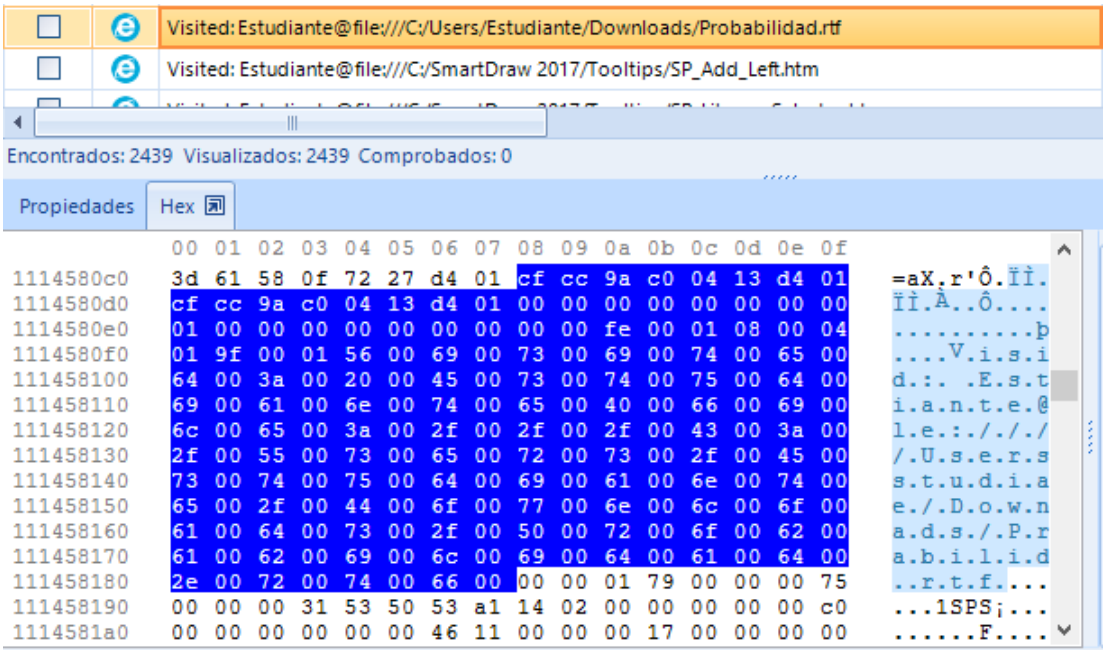


Figura 6.44: Registro de visita obtenido de la captura de memoria RAM.

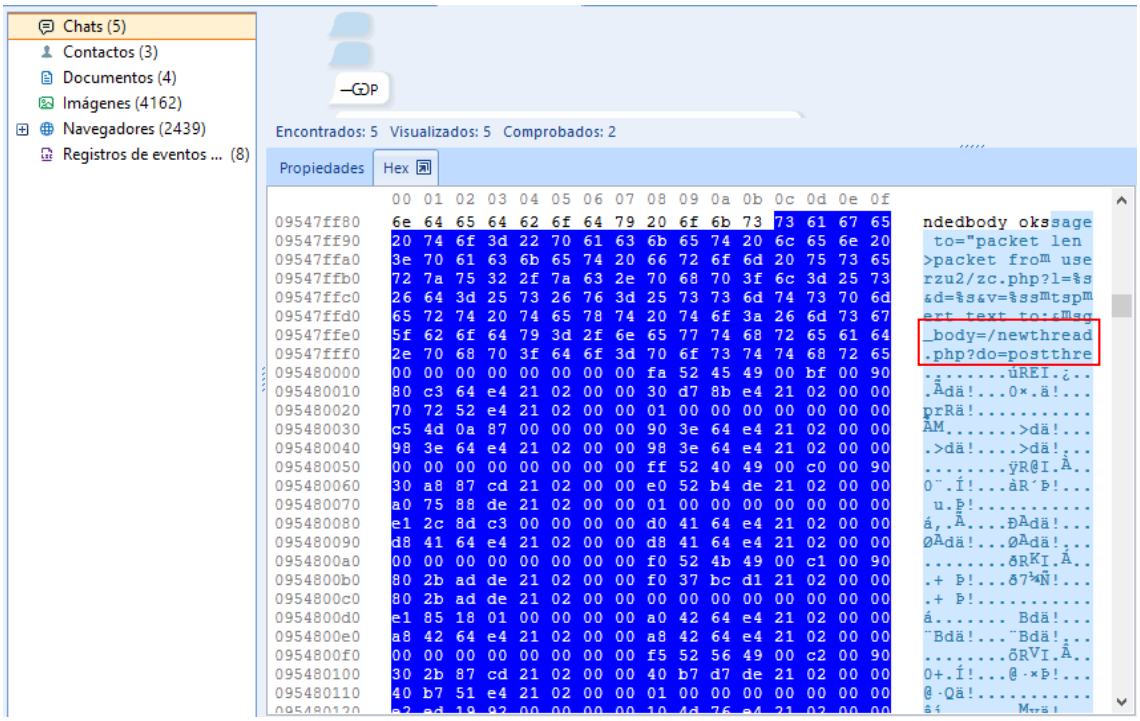


Figura 6.45: Chats almacenados en la captura de RAM.

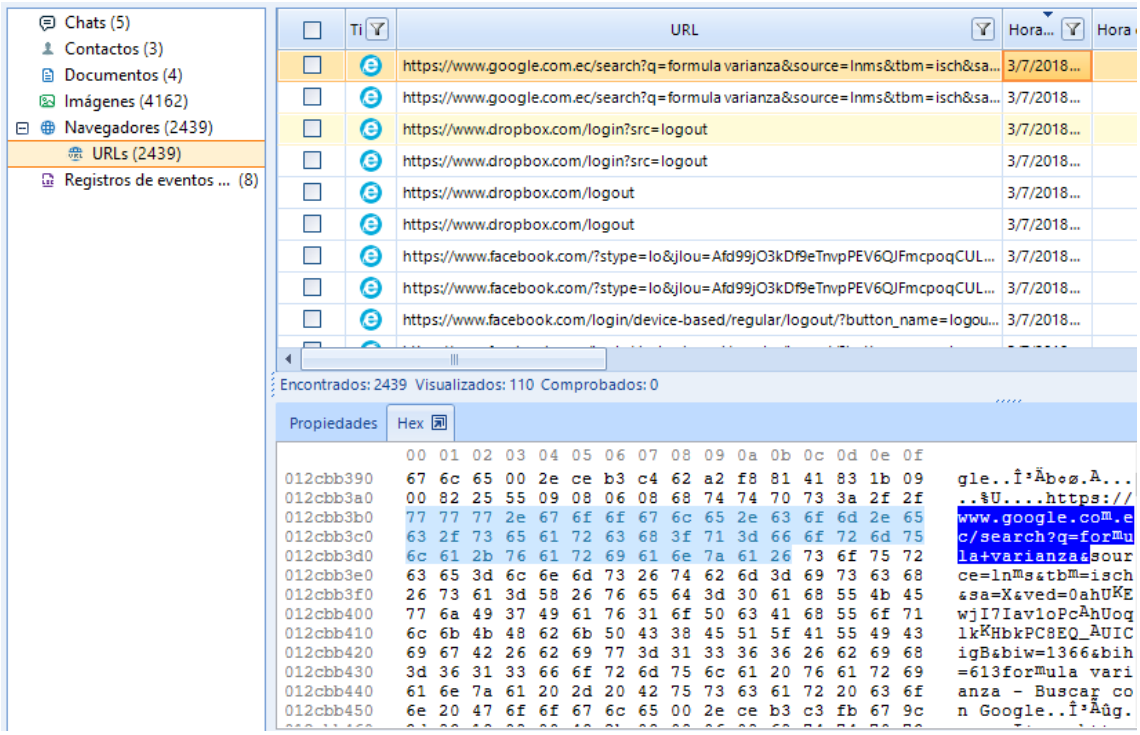


Figura 6.46: Registro de las URLs almacenadas en la captura de Memoria RAM.

Capítulo 7. Conclusiones

En este capítulo se recogen las conclusiones generales de este trabajo de titulación, las posibilidades de trabajos e investigación futura, así como los aportes científicos generados durante el mismo.

7.1 Conclusiones

En este trabajo se ha propuesto una metodología para el manejo de una investigación forense; enfocada en evidencia digital proveniente de entornos web, que ayudará a los investigadores a seguir un proceso de investigación, durante todas sus fases, basado en prácticas de expertos en el área y bajo el marco de estándares internacionales.

Para la elaboración de la metodología se han considerado guías provistas por expertos dentro del marco de los estándares ISO/IEC 27037 y 27042. Presentando a los investigadores actividades específicas y bien definidas para llevar a cabo este tipo de pericias.

La motivación principal de este trabajo de titulación es el contar con una metodología que permita llevar a cabo una investigación forense enfocada al manejo de la evidencia digital procedente de sitios web en el lado del cliente. Permitiendo al investigador llevar a cabo una investigación válida que no se vea limitada por temas de jurisdicción.

La informática forense es una ciencia capaz de aportar en gran medida al ámbito de la justicia en su afán de la búsqueda por la verdad de los hechos, siendo muy importante en el mundo actual con el incremento de la interconexión de ordenadores, en gran medida por la aparición de la web, facilitando a las personas acceder a recursos web a nivel mundial gracias al Internet.

Según los objetivos planteados en el primer capítulo:

1. Realizar un estudio del estado actual de la investigación, en cuanto a la identificación, recolección, preservación, análisis y presentación de la evidencia digital proveniente de entornos Web orientados al aprovisionamiento de servicios.
2. Proponer una metodología que permita la identificación, recolección, preservación, análisis y presentación de evidencia digital generada por el usuario en el ordenador local que utilizó una aplicación web.
3. Definir todos los artefactos y parámetros necesarios que serán utilizados durante la aplicación de la metodología.
4. Evaluar esta propuesta, a través de pruebas de concepto y/o casos de estudio.

Se puede decir que todos y cada uno de ellos han sido abordados y satisfechos:

Con respecto al objetivo 1, se realizó una revisión de literatura, sobre cómo se está llevando a cabo los procesos de una investigación forense de evidencia digital proveniente de entornos web enfocada en el lado del cliente.

Con respecto al objetivo 2, en el capítulo 4 se desarrolló la metodología basada en las fases de identificación, recolección, preservación, análisis y presentación. Incluyendo en cada una de las fases, actividades específicas que deben ser realizadas por el investigador de ser el caso.

Con respecto al objetivo 3, se planteó un escenario real, en el cual se puede identificar los artefactos web (cookies, cachés, historiales, etc.) que se deben tomar en cuenta en una investigación orientada a evidencia digital web, de la misma forma que se definió los parámetros de entrada para cada una de las fases de la metodología.

El objetivo 4, fue conseguido realizando una prueba de conceptos basada en el escenario propuesto y presentando los resultados más relevantes en un apartado.

Como se observa, los objetivos del trabajo de titulación fueron abarcados en su totalidad y a la vez que se logró un entendimiento en el tema acerca buenas prácticas en el manejo de la información dentro de una investigación forense, a continuación, se detallan las conclusiones más relevantes de este trabajo de titulación.

En el contexto actual no existe una guía íntegra que permita llevar una investigación forense basada en artefactos web en el lado del cliente, por lo que está metodología presenta una alternativa que permite a los investigadores llevar a cabo el proceso de pericia completo dentro de las normas ISO/IEC; donde el foco de la investigación sean actividades realizadas por el usuario en la web.

También cabe resaltar que existen casos particulares donde la información en el ordenador local es mínima; como en: sesiones privadas, sesiones portables, o cuando el usuario elimina artefactos. En estos casos el investigador debe optar por examinar de forma más profunda los artefactos existentes (si es que los hay), por ejemplo, en sesiones privadas es posible examinar el caché de las extensiones del navegador ya que estas no poseen la sesión privada. En caso de la sesión portable o si el usuario elimino gran cantidad de artefactos la solución puede encontrarse examinando la memoria volátil.

Se verificó también, la existencia de varias herramientas que permiten la recolección de artefactos web. Dentro de las cuales existen herramientas específicas de sistemas operativos o aplicaciones; donde, las aplicaciones

específicas optimizan los tiempos de ejecución pese a su incapacidad para abarcar los artefactos provenientes de diferentes aplicaciones. Por lo dicho es recomendable que el investigador identifique los artefactos web fundamentales de su investigación.

Otro aspecto para tener en cuenta es la factibilidad de desarrollar herramientas específicas para automatizar ciertas actividades de la investigación, pudiendo reducir recursos como el tiempo, como el script desarrollado en la fase de recolección de este trabajo de titulación.

7.2 Trabajos futuros

El trabajo presentado, contribuye una primera guía sobre el manejo local de la evidencia digital en ordenadores, este puede ser aplicado posteriormente a otros tipos de dispositivos como dispositivos móviles u otros dispositivos inteligentes que van apareciendo con los avances tecnológicos.

Este trabajo presenta un primer enfoque sobre la optimización del proceso de recolección, se podría continuar el estudio en este ámbito verificando si existen otras actividades dentro de una investigación forense que puedan ser optimizadas.

Otro trabajo a futuro será el estudio de como se está manejando la evidencia digital procedente de dispositivos en IoT y otros dispositivos inteligentes.

La propuesta de herramienta realizada también puede ser mejorada logrando mayo eficiencia si se consideran técnicas de paralelización.

Otro aspecto por considerar es la tendencia actual en cuanto a servicios forenses en la web. Lo que se busca es que la información web relevante en una investigación forense se encuentre disponible como un servicio propio de la aplicación web, a la cual los investigadores puedan solicitar el servicio y está a su vez devuelva la información íntegra y correcta al investigador. Un ejemplo de ello en la computación en la nube es FaaS, el servicio forense como un servicio.

7.3 Aporte científico

Durante el desarrollo de este trabajo de titulación se ha realizado dos contribuciones en modo de publicación que cubren aportación dos aportes de este trabajo de titulación. Las publicaciones fueron sometidas a un proceso de revisión y aceptadas en conferencias nacionales que publicaran los estudios en la IEEE y Springer. A continuación, se presentan estas y se detallan en que parte de este trabajo de titulación se vincula su contenido.

- Coronel, B.; Cedillo, P.; Campos, K.; Camacho, J.; Bermeo, A.: “A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective”, IEEE Ecuador Technical Chapters Meeting (IEEE ETCM 2018).

En este artículo se presentó una revisión sistemática de literatura (Capítulo 3), con esto se definió el estado actual de la investigación forense dirigida a evidencia digital proveniente de sitios web y se identificó la ausencia de una guía integra en esta área de estudio que dio origen a la metodología propuesta.

- Camacho, J; Campos, K; Cedillo, P; Coronel, B; Bermeo, A. “Forensics Analysis on Mobile Devices: A Systematic Mapping Study”, 6th Congreso Tecnologías de la Información y Comunicación del Ecuador (TIC-EC 2018).

Este artículo se presenta como un primer aporte a lo mencionado en la sección trabajos a futuro, en el cual se aborda un estado del arte en el área de los dispositivos móviles.

Las vistas preliminares de los artículos pueden ser encontrados en los anexos C y D respectivamente.

Referencias

About the Software y Systems Process Engineering Metamodel Specification Version 2.0. (2008). [Oficial]. Recuperado 21 de enero de 2018, de http://www.omg.org/spec/SPEM/About-SPEM/

Baca, M., Cosic, J., y Cosic, Z. (2013). Forensic analysis of social networks (case study). En *Proceedings of the ITI 2013 35th International Conference on Information Technology Interfaces* (pp. 219-223). https://doi.org/10.2498/iti.2013.0526

Bakshi, K. (2009). Cisco cloud computing-data center strategy, architecture, and solutions. *DOI= http://www. cisco. com/web/strategy/docs/gov/CiscoCloudComputing_WP. pdf*.

Benslimane, D., Dustdar, S., y Sheth, A. (2008). Services Mashups: The New Generation of Web Applications. *IEEE Internet Computing*, *12*(5), 13-15. https://doi.org/10.1109/MIC.2008.110

Bhosale, D. V., Mitkal, P. K., Pawar, R. N., y Paranjape, R. S. (2016). Review on Computer Forensic. *Training*, *2*(01).

Casey, E. (2001). *Handbook of Computer Crime Investigation: Forensic Tools and Technology*. Elsevier.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Academic Press.

Castellano, G., y Fanelli, A. M. (2009). *Web Personalization in Intelligent Environments*. Springer.

Castiglione, A., Cattaneo, G., y Santis, A. D. (2011). A Forensic Analysis of Images on Online Social Networks. En *2011 Third International Conference on Intelligent Networking and Collaborative Systems* (pp. 679-684). https://doi.org/10.1109/INCoS.2011.17

Chen, L., Xu, L., Yuan, X., y Shashidhar, N. (2015). Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. En *2015 International Conference on Computing, Networking and Communications (ICNC)* (pp. 1132-1136). https://doi.org/10.1109/ICCNC.2015.7069509

Choo, K. K. R., Esposito, C., y Castiglione, A. (2017). Evidence and Forensics in the Cloud: Challenges and Future Research Directions. *IEEE Cloud Computing*, *4*(3), 14-19. https://doi.org/10.1109/MCC.2017.39

Chow, K. P., Chong, C. F., Lai, K. Y., Hui, L. C. K., Pun, K. H., Tsang, W. W., y Chan, H. W. (2005). Digital evidence search kit. En *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)* (pp. 187-194). https://doi.org/10.1109/SADFE.2005.10

Council, C. S. C. (2013). *Cloud security standards: what to expect y what to negotiate*. October.

CSRC - Glossary - Web Browser. (2017). [Glosario]. Recuperado 8 de mayo de 2018, de https://csrc.nist.gov/Glossary/?term=2447#AlphaIndexDiv

Domingues, P., y Frade, M. (2016). Digital Forensic Artifacts of the Cortana Device Search Cache on Windows 10 Desktop. En *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 338-344). https://doi.org/10.1109/ARES.2016.44

Farina, J., Scanlon, M., Le-Khac, N. A., y Kechadi, M. T. (2015). Overview of the Forensic Investigation of Cloud Services. En *2015 10th International Conference on Availability, Reliability and Security* (pp. 556-565). https://doi.org/10.1109/ARES.2015.81

Galante, G., y Bona, L. C. E. de. (2012). A Survey on Cloud Computing Elasticity. En *Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility*

and Cloud Computing (pp. 263–270). Washington, DC, USA: IEEE Computer Society. https://doi.org/10.1109/UCC.2012.30

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, S64-S73. https://doi.org/10.1016/j.diin.2010.05.009

Guo, H., Jin, B., y Huang, D. (2010). Research and Review on Computer Forensics. En *Forensics in Telecommunications, Information, and Multimedia* (pp. 224-233). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23602-0_21

Gupta, D., y Mehtre, B. M. (2013). Recent Trends in Collection of Software Forensics Artifacts: Issues and Challenges. En *Security in Computing and Communications* (pp. 303-312). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40576-1_30

Hatole, P. P., y Bawiskar, D. S. K. (2017). Literature Review of Email Forensics. *Imperial Journal of Interdisciplinary Research*, *3*(4). Recuperado de http://imperialjournals.com/index.php/IJIR/article/view/4555

Hausenblas, M. (2011). *Building Scalable and Smart Multimedia Applications on the Semantic Web*. GRIN Verlag.

Held, G. (2000). *Server Management*. CRC Press.

Helfgott, J. B. (2008). *Criminal Behavior: Theories, Typologies and Criminal Justice*. SAGE.

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). Metodología de la investigación. Sexta Edición. Editorial Mc Graw Hill. México. *Metodología de la Investigación. 6a Edición, Mc Graw Hill, México*.

Hibbard, E. (2014). ELECTRONIC DISCOVERY STANDARDIZATION, *12*, 19.

Howden, C., Liu, L., Ding, Z., Zhan, Y., y Lam, K. P. (2013). Moments in Time: A Forensic View of Twitter. En *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing* (pp. 899-908). https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.157

ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services. (2015). [Oficial]. Recuperado 14 de mayo de 2018, de https://www.iso.org/standard/43757.html

ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital

evidence. (2012). [Oficial]. Recuperado 14 de septiembre de 2017, de https://www.iso.org/standard/44381.html

ISO/IEC 27041:2015 - Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method. (2015). [Oficial]. Recuperado 14 de mayo de 2018, de https://www.iso.org/standard/44405.html

ISO/IEC 27042:2015- Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence. (2015). [Oficial]. Recuperado 14 de septiembre de 2017, de https://www.iso.org/standard/44406.html

ISO/IEC 27050-3:2017 - Information technology -- Security techniques -- Electronic discovery -- Part 3: Code of practice for electronic discovery. (2017). [Oficial]. Recuperado 30 de mayo de 2018, de https://www.iso.org/standard/66231.html

Jang, Y.-J., y Kwak, J. (2015). Digital forensics investigation methodology applicable for social network services. *Multimedia Tools and Applications*, *74*(14), 5029-5040. https://doi.org/10.1007/s11042-014-2061-8

Jara, Di., y Cedillo, P. (2017). Towards the Definition of Security Vulnerabilities in Mobile Cloud Computing.

Kaur, M., Kaur, N., y Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering*, *5*(1), 23–28.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews. *Keele, UK, Keele Univ.*, *33*.

Koreneff, I., y Sims-McLean, K. (2005). *Information Technology*. Pascal Press.

Lee, S., Lee, S., Lim, J., y Kim, H. (2005). Digital evidence collection process in integrity and memory information gathering. En *First International Workshop on Systematic Approaches to Digital Forensic Engineering* (pp. 236-247). Los Alamitos, CA, USA: IEEE Computer Society. https://doi.org/10.1109/SADFE.2005.9

Levinson, A., Stackpole, B., y Johnson, D. (2011). Third Party Application Forensics on Apple Mobile Devices. En *2011 44th Hawaii International Conference on System Sciences* (pp. 1-9). https://doi.org/10.1109/HICSS.2011.440

Lewis, G. A. (2013). Role of Standards in Cloud-Computing Interoperability. En *2013 46th Hawaii International Conference on System Sciences* (pp. 1652-1661). https://doi.org/10.1109/HICSS.2013.470

Li, Z., Tang, C., Hu, J., y Chen, Z. (2015). Vulnerabilities Scoring Approach for Cloud SaaS. En *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)* (pp. 1339-1347). https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.242

Mahaju, S., y Atkison, T. (2017). Evaluation of Firefox Browser Forensics Tools. En *Proceedings of the SouthEast Conference* (pp. 5–12). New York, NY, USA: ACM. https://doi.org/10.1145/3077286.3077310

Majeed, A., Zia, H., Imran, R., y Saleem, S. (2015). Forensic analysis of three social media apps in windows 10. En *2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET)* (pp. 1-5). https://doi.org/10.1109/HONET.2015.7395419

Marturana, F., Me, G., y Tacconi, S. (2012). A Case Study on Digital Forensics in the Cloud. En *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 111-116). https://doi.org/10.1109/CyberC.2012.26

Matsumoto, S., y Sakurai, K. (2014). Acquisition of Evidence of Web Storage in HTML5 Web Browsers from Memory Image. En *2014 Ninth Asia Joint Conference on Information Security* (pp. 148-155). https://doi.org/10.1109/AsiaJCIS.2014.30

Mehreen, S., y Aslam, B. (2015). Windows 8 cloud storage analysis: Dropbox forensics. En *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 312-317). https://doi.org/10.1109/IBCAST.2015.7058522

Mell, P. M., y Grance, T. (2011). The NIST Definition of Cloud Computing. *Special Publication (NIST SP) - 800-145*. Recuperado de https://www.nist.gov/publications/nist-definition-cloud-computing

Miranda Lopez, E., Moon, S., y Park, J. (2016). Scenario-Based Digital Forensics Challenges in Cloud Computing. *Symmetry*, *8*(10), 107. https://doi.org/10.3390/sym8100107

Mirza, F. (2008). Looking for digital evidence in Windows. En *2008 International Symposium on Biometrics and Security Technologies* (pp. 1-7). https://doi.org/10.1109/ISBAST.2008.4547659

Morioka, E., y Sharbaf, M. S. (2016). Digital forensics research on cloud computing: An investigation of cloud forensics solutions. En *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). https://doi.org/10.1109/THS.2016.7568909

Nair, A. S. V., y Ajeena, B. A. S. (2014). A Log Based Strategy for Fingerprinting and Forensic Investigation of Online Cyber Crimes. En *Proceedings of the 2014 International Conference on Interdisciplinary Advances in Applied Computing* (pp. 7:1–7:5). New York, NY, USA: ACM. https://doi.org/10.1145/2660859.2660912

Nalawade, A., Bharne, S., y Mane, V. (2016). Forensic analysis and evidence collection for web browser activity. En *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)* (pp. 518-522). https://doi.org/10.1109/ICACDOT.2016.7877639

Oh, J., Lee, S., y Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation*, *8*(Supplement), S62-S70. https://doi.org/10.1016/j.diin.2011.05.008

Ohana, D. J., y Shashidhar, N. (2013). Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions. En *Proceedings of the 2013 IEEE Security and Privacy Workshops* (pp. 135–142). Washington, DC, USA: IEEE Computer Society. https://doi.org/10.1109/SPW.2013.18

Raju, B. K. S. P. K., y Geethakumari, G. (2016). An advanced forensic readiness model for the cloud environment. En *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 765-771). https://doi.org/10.1109/CCAA.2016.7813819

Reyes, A., Brittson, R., O'Shea, K., y Steele, J. (2011). *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*. Elsevier.

Ricca, F., y Tonella, P. (2001). Analysis and Testing of Web Applications. En *Proceedings of the 23rd International Conference on Software Engineering* (pp. 25–34). Washington, DC, USA: IEEE Computer Society. Recuperado de http://dl.acm.org/citation.cfm?id=381473.381476

Roussev, V., y McCulley, S. (2016). Forensic analysis of cloud-native artifacts. *Digital Investigation*, *16*(Supplement), S104-S113. https://doi.org/10.1016/j.diin.2016.01.013

Ruan, K., Carthy, J., Kechadi, T., y Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation*, *10*(1), 34-43. https://doi.org/10.1016/j.diin.2013.02.004

Said, H., Mutawa, N. A., Awadhi, I. A., y Guimaraes, M. (2011). Forensic analysis of private browsing artifacts. En *2011 International Conference on Innovations in Information Technology* (pp. 197-202). https://doi.org/10.1109/INNOVATIONS.2011.5893816

Saleem, S., Popov, O., y Dahman, R. (2011). Evaluation of security methods for ensuring the integrity of digital evidence. En *2011 International Conference on Innovations in Information Technology* (pp. 220-225). https://doi.org/10.1109/INNOVATIONS.2011.5893821

Sang, T. (2013). A Log Based Approach to Make Digital Forensics Easier on Cloud Computing. En *2013 Third International Conference on Intelligent System Design and Engineering Applications* (pp. 91-94). https://doi.org/10.1109/ISDEA.2012.29

Simou, S., Kalloniatis, C., Kavakli, E., y Gritzalis, S. (2014). Cloud Forensics Solutions: A Review. En *Advanced Information Systems Engineering Workshops* (pp. 299-309). Springer, Cham. https://doi.org/10.1007/978-3-319-07869-4_28

Sivaprasad, A., y Jangale, S. (2012). A complete study on tools amp; techniques for digital forensic analysis. En *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)* (pp. 881-886). https://doi.org/10.1109/ICCEET.2012.6203877

Subhash, C. Y. (2009). *Introduction To Client Sever Computing*. New Age International.

Tipton, H. F. (2014). *Information Security Management Handbook, Fourth Edition*. CRC Press.

Veber, Jaromír, y Klíma, T. (2014). Influence of Standards ISO 27000 Family on Digital Evidence Analysis. *Proceedings of the 22nd Interdisciplinary Information Management Talks*, 103–114.

Veber, Jaromír, y Klima, T. (2015). *MAPPING OF ISO 27000 DIGITAL EVIDENCE TO PROCESSES OF DIGITAL FORENSICS LAB*.

Veber, Jaromir, y Smutny, Z. (s. f.). Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic, 7.

Wang, Y. (2010). Study on Supervision of Integrity of Chain of Custody in Computer Forensics. En *Forensics in Telecommunications, Information, and*

Multimedia (pp. 200-206). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23602-0_19

Zawoad, S., y Hasan, R. (2016). Trustworthy Digital Forensics in the Cloud. *Computer*, *49*(3), 78-81.

Anexos

Anexo A: Código de la propuesta de herramienta.

Funciones.py

```
# To change this license header, choose License Headers in Project Properties.
# To change this template file, choose Tools | Templates
# and open the template in the editor.
import shutil
import os
import glob
def GetHashofDirs(directory, archivo, verbose=0):
  import hashlib
  contador =0
  SHAhash = hashlib.md5()
  if not os.path.exists (directory):
    return -1
  try:
    for root, dirs, files in os.walk(directory):

      for names in files:
        if verbose == 1:
          print 'Hashing', names
        filepath = os.path.join(root,names)
        try:
          f1 = open(filepath, 'rb')
```

```
      except:
        # You can't open the file for some reason
        f1.close()
        continue

      while 1:
        # Read file in as little chunks
        buf = f1.read(4096)
        if not buf : break
        SHAhash.update(hashlib.md5(buf).hexdigest())
      f1.close()
      contador=contador+1

except:
  import traceback
  # Print the stack traceback
  traceback.print_exc()
  return -2
f=open(archivo,"a")
if contador>1:
  f.write("\n"+directory +"/: "+ SHAhash.hexdigest())
  f.close
  print "Archivo de valores Hash Registrado"
else:
    f.write("\n"+directory +": "+ SHAhash.hexdigest())
    f.close
```

```
      print "Archivo de valores Hash Registrado"
  return SHAhash.hexdigest()
def copiarDirectorio(directorio,destino):
    shutil.copytree(directorio,destino,symlinks=False, ignore=None)
    return
def copiarArchivo(archivo,destino):
    shutil.copytree(archivo,destino)
    return
def definirChromePath():
    try:
        path=glob.glob("C:/Users/*/AppData/Local/Google/Chrome/User
Data/Default")[0]
        return path
    except:
        import traceback
    # Print the stack traceback
        traceback.print_exc()
        return "0"
def definirMozillaPath():
    try:
        return
glob.glob("C:/Users/*/AppData/Roaming/Mozilla/Firefox/Profiles/*")[0]
    except:
        return 0
def cacheMozillaPath():
    try:
        return glob.glob("C:\Users\*\AppData\Local\Mozilla\Firefox\Profiles\*")[0]
```

```
    except:
        return 0;
```

Capturer.py

```
# To change this license header, choose License Headers in Project Properties.
# To change this template file, choose Tools | Templates
# and open the template in the
import shutil
import os
from time import time #importamos la función time para capturar tiempos
import funciones
ch=0
fx=0
pathChrome= funciones.definirChromePath()
tiempo_inicial = time()
if  os.path.exists(pathChrome):
    print "El navegador Google Chrome ha sido detectado"
    ch=1
    #Se crea un directorio en el dispositvo para almacenar sus artefactos
    if os.path.exists(os.getcwd()+"/ChromeData"):
        shutil.rmtree(os.getcwd()+"/ChromeData")
    os.makedirs(os.getcwd()+"/ChromeData")#directorio objetivo
    #Empezamos la recoleccion
    #Las cookies
    try:

shutil.copy(os.path.join(pathChrome+"/Cookies"),os.getcwd()+"/ChromeData/Cookies")
```

```
        print "Hash de Chrome Cookies:"+funciones.GetHashofDirs(os.getcwd()+"/ChromeData/Cookies","HashValuesCrhome.txt" , 1);
    except:
        print "Algunos archivos no pueden ser accesados... Cookies"
        import traceback
    # Print the stack traceback
        traceback.print_exc()
    try:
        shutil.copy(os.path.join(pathChrome+"/Cookies-journal"),os.getcwd()+"/ChromeData/Cookies-Journal")
        print "Hash de Chrome Cookies-Journal:"+funciones.GetHashofDirs(os.getcwd()+"/ChromeData/Cookies-Journal","HashValuesCrhome.txt", 1);
    except:
        print "Algunos archivos no pueden ser accesados...Cookies Journal"
        #historial
    try:

shutil.copy(os.path.join(pathChrome+"/History"),os.getcwd()+"/ChromeData/History")
        print "Hash de Chrome Historial:"+funciones.GetHashofDirs(os.getcwd()+"/ChromeData/History","HashValuesCrhome.txt", 1);
    except:
        print "Algunos archivos no pueden ser accesados...History"
        #historiales de loggins
    try:
        shutil.copy(os.path.join(pathChrome+"/Login Data"),os.getcwd()+"/ChromeData/Loggins")
```

```
    print "Hash de Chrome Cache:"+funciones.GetHashofDirs(os.getcwd()+"/ChromeData/Loggins","HashValuesCrhome.txt", 1);

    except:

        print "Algunos archivos no pueden ser accesados...Loggins"

#rescatamos las caches del navegador

    try:


shutil.copytree(os.path.join(pathChrome+"/Cache"),os.getcwd()+"/ChromeData/Cache",symlinks=False, ignore=None)

    except:

        print "Archivos de la Cache no permitidos"

    try:


shutil.copytree(os.path.join(pathChrome+"/GPUCache"),os.getcwd()+"/ChromeData/CacheGPU",symlinks=False, ignore=None)

    except:

        print "Algunos archivos Cache GPU no estan permitidos"

    #Obtenemos los valores hash!

    print "Hash de Chrome Cache:"+funciones.GetHashofDirs(os.getcwd()+"/ChromeData/Cache","HashValuesCrhome.txt", 1);

    print "Hash de Chrome CacheGPU:"+funciones.GetHashofDirs(os.getcwd()+"/ChromeData/CacheGPU","HashValuesCrhome.txt", 1);

    print("Proceso Chrome terminado")

else:

    print "El navegador Google Chrome no ha sido detectado"


#####################################################################################################
```

```
##############################################Mozilla#####################
#############################

#Vamos con MOzila

moziPath=funciones.definirMozillaPath()

if os.path.exists(moziPath):

    print "Se ha detectado el navegador Mozila>>>"

    fx=1

    if os.path.exists(os.getcwd()+"/FirefoxData"):

        shutil.rmtree(os.getcwd()+"/FirefoxData")

    os.makedirs(os.getcwd()+"/FirefoxData")

    #Recoger Cookies

    try:


shutil.copy(os.path.join(moziPath+"/cookies.sqlite"),os.getcwd()+"/FirefoxData/c
ookies.sqlite")

        print "Hash de Fx
cookies:"+funciones.GetHashofDirs(os.getcwd()+"/FirefoxData/cookies.sqlite","
HashValuesFirefox.txt", 1);

    except:

        import traceback

    # Print the stack traceback

        traceback.print_exc()

        print "No se pudo acceder a las cookies de Fx"

    #vamos por el historial....

    try:


shutil.copy(os.path.join(moziPath+"/formhistory.sqlite"),os.getcwd()+"/FirefoxDat
a/formhistory.sqlite")
```

```
        print "Hash de Fx historial:"+funciones.GetHashofDirs(os.getcwd()+"/FirefoxData/formhistory.sqlite","HashValuesFirefox.txt", 1);
    except:
        print "No se pudo acceder al historial de Fx"

    #VRecolectar Caches!
    try:

shutil.copytree(os.path.join(moziPath+"/storage/default"),os.getcwd()+"/FirefoxData/CacheFireFoxApps",symlinks=False, ignore=None)
    except:
        print "Archivos de la Cache no permitidos"
    print "Hash de Fx Cache:"+funciones.GetHashofDirs(os.getcwd()+"/FirefoxData/CacheFireFoxApps","HashValuesFirefox.txt", 1);
    cachePath=funciones.cacheMozillaPath()
    l=["cache2", "jumListCache","OfflineCache","safebrowsing","startupCache"]
    for i in l:
        try:
            print i+ " extrayendo...."

shutil.copytree(os.path.join(cachePath+"/"+i),os.getcwd()+"/FirefoxData/"+i,symlinks=False, ignore=None)
        except:
            print "No se pudo acceder a cierta cache de Fx"
            continue
    for j in l:
```

```
print(funciones.GetHashofDirs(os.getcwd()+"/FirefoxData/"+j,"HashValuesFirefox.txt", 1));

        print j

    print "Analisis Firefox terminado"

else:

    print "No se ha detectado el navegador Firefox..."


tiempoFinal=time()

print("**********************************************************************************************************************")

print "Navegadores detectados:"

if ch==1:

    print("Google Chrome")

if fx==1:

    print("Firefox Mozilla")

tiempoEjecucion=tiempoFinal-tiempo_inicial

#raw_input("Ejecucion completa en: "+ tiempoEjecucion+"pulse una tecla para continuar")
```

Anexo B: Informe Pericial

"INFORME PERICIAL"

1. DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA

No. de Proceso	001
Nombre y Apellido de la o el Perito	Bryan Daniel Coronel Tapia
Dirección de Contacto	Guantánamo y Ecuador
Teléfono fijo de contacto	072817427
Teléfono celular de contacto	0984272523
Correo electrónico de contacto	bryan.coronel@ucuenca.edu.ec

2. PARTE DE ANTECEDENTES,

He sido llamado como perito por parte del docente de la asignatura de Probabilidad Ing. Esteban Mora; para analizar las actividades realizadas desde el ordenador C001 del centro de cómputo dos de la facultad de Ingeniería.

El docente ha solicitado al investigador verificar que actividades realizó el estudiante en Internet en su máquina en el periodo de tiempo de las 13:00 y el momento que el estudiante se retira 14:50.

3. PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE,

Yo, Bryan Coronel con experiencia de 5 años en el manejo de tecnologías como son, tratamiento de información, análisis de imágenes, tratamiento de evidencia digital, entre otros; que dan fe al correcto cumplimiento del encargo encomendado en orden a efectuar una pericia formulo el siguiente **Diseño de Pericia** basado en la metodología para llevar una investigación basada evidencia web**,** conforme la siguiente pauta de trabajo y desarrollo que determinará los objetivos perseguidos.

Diseño de Pericia:

- Identificación y preparación de equipos.
- Recolección de Información volátil.
- Realizar imágenes forenses.
- Recolección de artefactos web.
- Análisis de artefactos web.

4. PARTE DE CONCLUSIONES,

Una vez analizados los antecedentes y tomando en base lo especificado en las preguntas respectivas este perito puede concluir lo siguiente:

PREGUNTA

- Pericia informática respecto a las actividades ejecutadas por el estudiante en Internet en el periodo de la prueba de probabilidad.

CONCLUSIÓN:

Luego del análisis realizado se identificaron las siguientes actividades:

- Se logró detectar que hubo acceso a aplicaciones web diferentes a la plataforma elegida para rendir la prueba de probabilidad (Facebook, Google y Dropbox) mediante el navegador web Google Chrome.
- Se verificó que se inició sesión en Facebook y Dropbox con el correo bryantc_hjj@hotmail.com
- Las búsquedas que se realizaron en Google fueron identificadas con las siguientes cadenas de caracteres: “desviación estandar”, “formula varianza”, “probabilidad”.
- Se verificó la descarga de tres archivos procedentes de Dropbox.
- Se verificó que el archivo Probabilidad.rtf fue accedido

Esto de acuerdo a lo solicitado en la pericia.

5. PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO,

Luego de la investigación de las tecnologías requeridas para atender la solicitud y realizar las pruebas, procedo a presentar mi opinión técnica a cada pregunta formulada al momento de requerir esta pericia.

Se identifica el ordenador objeto de la investigación, y se lo identifica con el código "C001" con número de serie MXL41213Y0, como se muestra en la Figura 1.

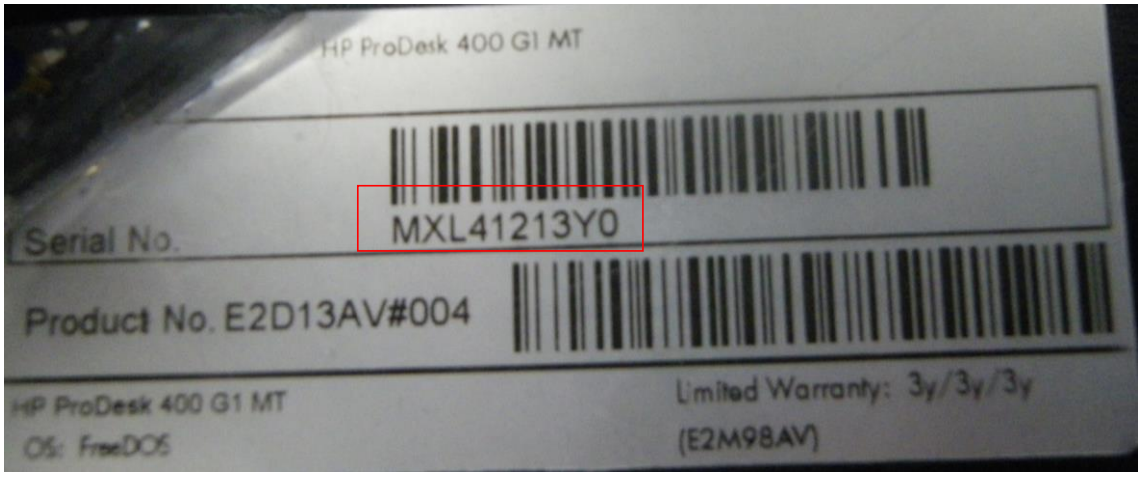


Figura 1: Número de serie del ordenador objeto de la investigación.

Al estar el ordenador encendido, se procede a capturar la información volátil junto con sus valores hash para salvaguardar la integridad, como se muestra en la Figura 2.

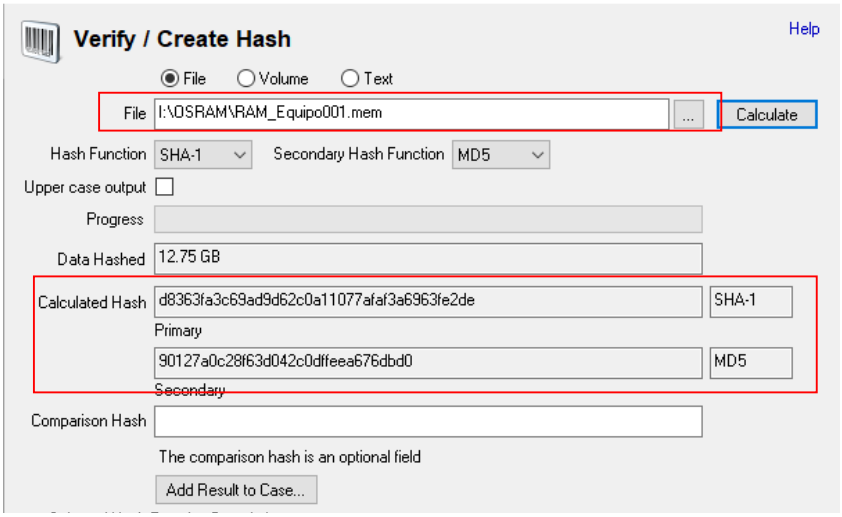


Figura 2: Calculo de funciones hash de la captura de memoria volátil.

De la misma manera se realiza una imagen del disco duro para su posterior análisis. El proceso se evidencia en la Figura 3.

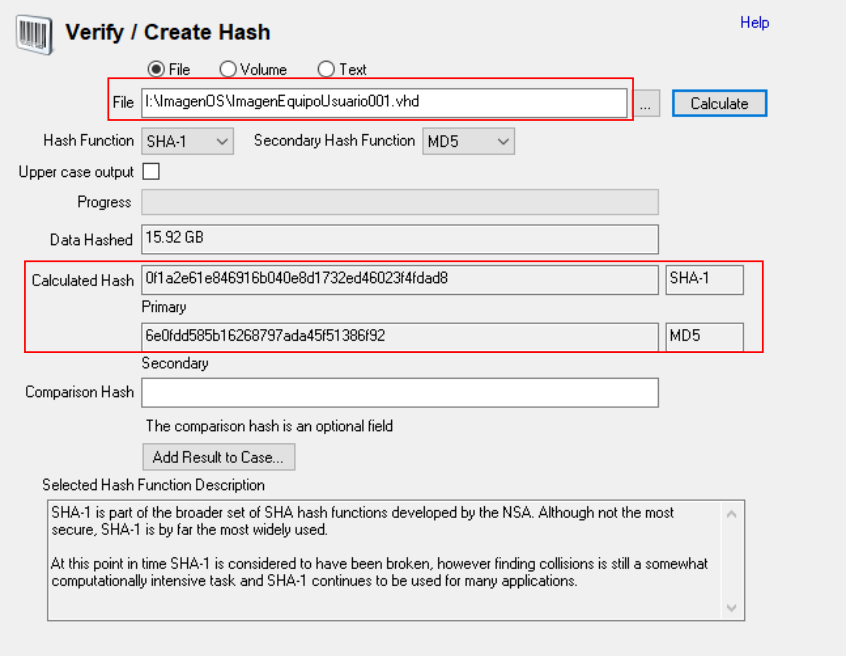


Figura 3: Calculo de funciones has de la imagen del disco duro.

A continuación, se montan las imágenes obtenidas en este caso hemos utilizado el software OS Forensics para este proceso; validando previamente su integridad, se procede a recolectar la información digital procedente de sitios web: cachés, cookiés, historiales. El proceso de recolección de la información específica se evidencia en la Figura 4.

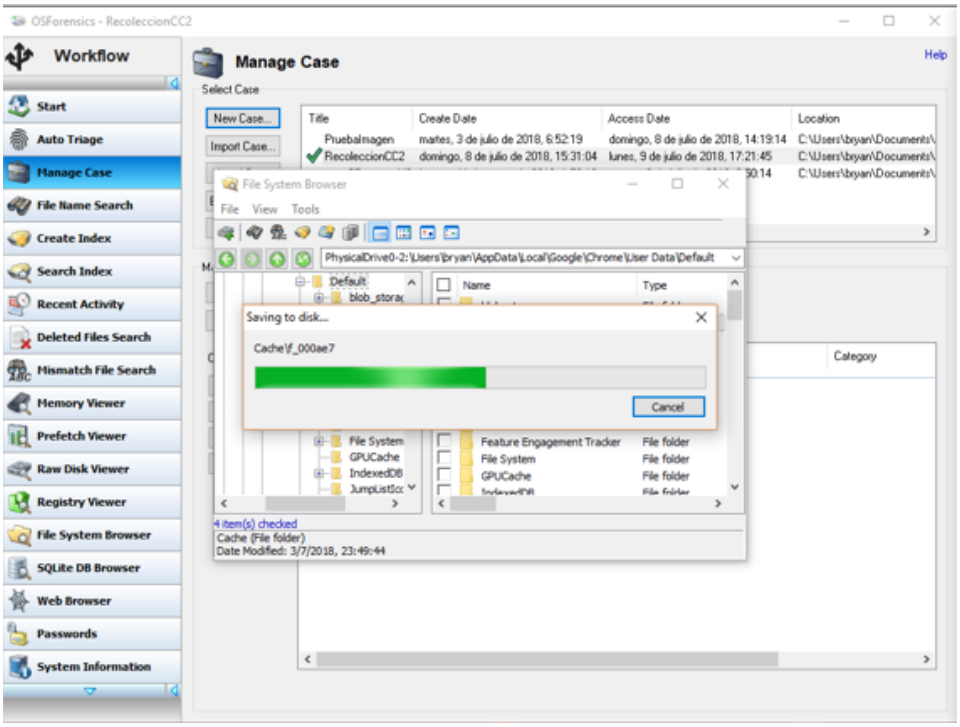


Figura 4: Adquisición de artefactos web

Con la información recolectada se procedió a almacenar junto con su firma digital para garantizar su integridad en caso de ser necesario, el proceso de creación de la forma digital se evidencia en la Figura 5.

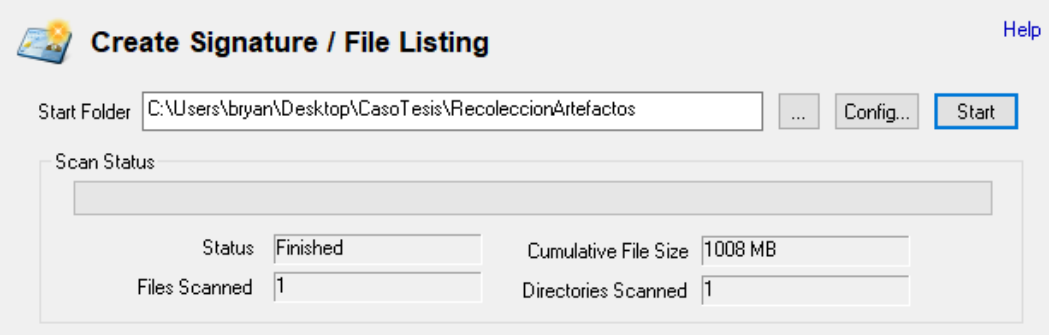


Figura 5: Creación de firma digital para la información recolectada.

Para el análisis de la evidencia se han empleado las herramientas: OS Forensics para montar la información recolectada, Autopsy para el análisis de cada uno de los artefactos, Evidence Center by Belkasoft para el análisis de la memoria volátil.

Empleando Autopsy se logró encontrar cookies que señalan el acceso y descarga de archivos del sitio web Dropbox accedidas en el horario de la prueba, como se aprecian en las figuras 6 y 7 respectivamente.

Result: 11 of 376 Result — Web Cookies

Type	Value
URL	www.dropbox.com
Date/Time	2018-07-03 14:42:06
Name	seen-sl-signup-modal
Value	
Program Name	Chrome
Domain	www.dropbox.com
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774883

Figura 6: Cookie de suscripción del sitio web Dropbox.

Result: 349 of 376 Result — Web Cookies

Type	Value
URL	www.dropbox.com
Date/Time	2018-07-03 14:42:06
Name	seen-sl-download-modal
Value	
Program Name	Chrome
Domain	www.dropbox.com
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774545

Figura 7: Cookie para el modo descarga del sitio web Dropbox.

También fueron encontrados cookies pertenecientes a los sitios web Google y Facebook, como se aprecia en la Figura 8.

Cookies	www.google.com.ec	2018-07-03 14:40:06 COT
Cookies	.facebook.com	2018-07-03 14:40:06 COT

Figura 8: Cookies encontrados de Google y Facebook.

También se encontró cookies utilizadas por el sitio elegido para registrar la prueba de probabilidad como se aprecia en la Figura 9.

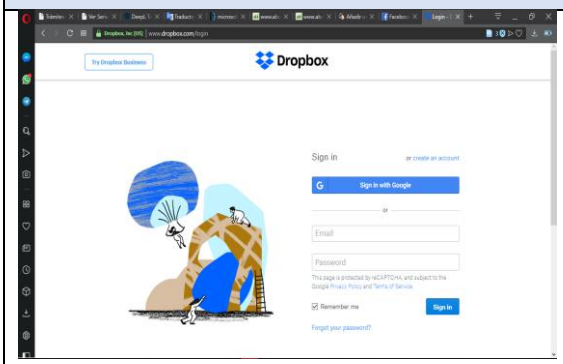
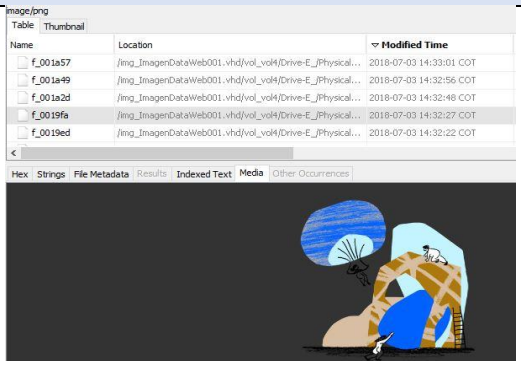
Result: 345 of 376 Result Web Cookies

Type	Value
URL	evirtual.ucuenca.edu.ec
Date/Time	2018-07-03 14:34:21
Name	MoodleSession
Value	
Program Name	Chrome
Domain	evirtual.ucuenca.edu.ec
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/Cookies
Artifact ID	-9223372036854774549

Figura 9: Cookie de sesión procedente del Evirtual.

Luego se procedió al análisis de las cachés de navegación encontrando en primer lugar imágenes relacionadas con sitios web, como la que se muestra en la Tabla 1 procedente del sitio web Dropbox.

Tabla 1: Elemento original y encontrado en la caché.

Sitio Web	Elemento Cache
	

De manera posterior se analizó los historiales de las aplicaciones de navegación encontrando:

En primer lugar, el historial de búsquedas realizadas en Google durante el periodo del examen, el mismo que se muestra en la Figura 10.

Listing
Web Search
Table | Thumbnail

Source File	Domain	Text	Program Name	Date Accessed	Data Source
History	www.google.com.ec	desviacion estandar	Chrome	2018-07-03 14:40:17 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:40:11 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:10 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:07 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:06 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:04 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:03 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:02 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:02 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	formula varianza	Chrome	2018-07-03 14:34:02 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	probabilidad	Chrome	2018-07-03 14:33:56 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	probabilidad	Chrome	2018-07-03 14:33:53 COT	ImagenDataWeb001.vhd
History	www.google.com.ec	dota 2 leaderboards	Chrome	2018-07-02 18:41:46 COT	ImagenDataWeb001.vhd

Figura 10: Historial de búsquedas en Google.

Revisando el historial de navegación se detectan los siguientes hechos relevantes: se muestran en la Tabla 2):

En el evento E1, se registra el acceso al curso virtual “PROBABILIDAD EIET/G1” en la plataforma Evirtual a las 14:31:07.

En el evento E2, se registra un intento de ingreso en la red social Facebook a las 14:31:49.

Seguido del evento E2, en el evento E3 se registra un intento de acceso a la aplicación web Dropbox a las 14:32:27.

Por su parte en el evento E4, se registra la visita de un perfil de Facebook cuyo nombre es “Bryan Coronel” a las 14:32:58.

De manera posterior en el evento E5, se verifica que el estudiante accedió a la prueba colocada en la plataforma virtual a las 14:34:21.

En el evento E6, se registra la finalización de sesión en la aplicación web Dropbox a las 14:40:06.

Finalmente, en el evento E7, se verifica la existencia de búsquedas en Google a las 14:40:11.

Tabla 2: Eventos relevantes del historial de navegación procedente de Autopsy

ID	Fecha	URL	Título
E1	2018-07-03 14:31:07	https://evirtual.ucuenca.edu.ec/course/view.php?id=7029	Course: PROBABILIDAD EIET /G1
E2	2018-07-03 14:31:49	https://www.facebook.com/login.php?login_attempt=1ylwv=111	Facebook
E3	2018-07-03 14:32:27	https://www.dropbox.com/login?cont=https%3A%2F%2Fwww.dropbox.com%2Fsh%2Fjz9a5cvemy3q02i%2FAACZLbTCQI37oRY8CERqz26Ga%3Fdl%3D0	Inicia sesión - Dropbox
E4	2018-07-03 14:32:58	https://www.facebook.com/CoR0TApiA	Bryan Coronel
E5	2018-07-03 14:34:21	https://evirtual.ucuenca.edu.ec/mod/quiz/attempt.php?attempt=16347	Prueba Capítulos 5y6
E6	2018-07-03 14:40:06	https://www.dropbox.com/login?src=logout	Login - Dropbox
E7	2018-07-03 14:40:11	https://www.google.com.ec/search?q=formula+varianzaysource=lnmsytbm=ischysa=Xyved=0ahUKEwjI7Iav1oPcAhUoqlkKHbkPC8EQ_AUICigBybiw=1366ybih=613	formula varianza - Buscar con Google

Analizando los accesos se verifico un acceso a Dropbox con el correo electrónico bryantc_hjj@hotmail.com, como se muestra en la Figura 11.

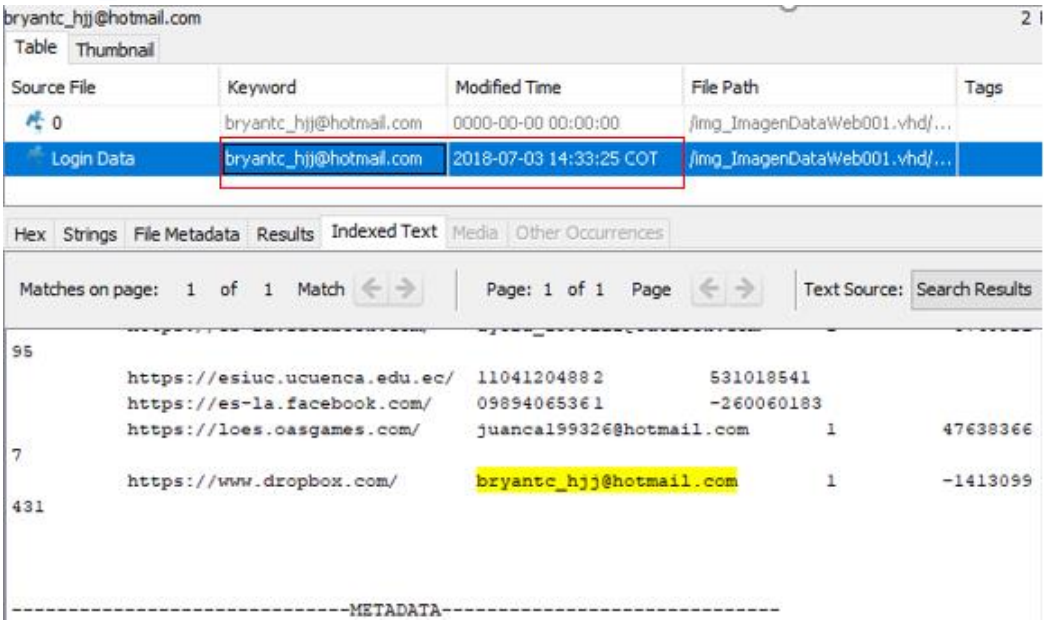


Figura 11: Identificación de acceso del correo bryantc_hjj@hotmail.com.

En el historial de descargas, se verifico la descarga de tres archivos durante la realización de la prueba, como se aprecia en la Figura 12.

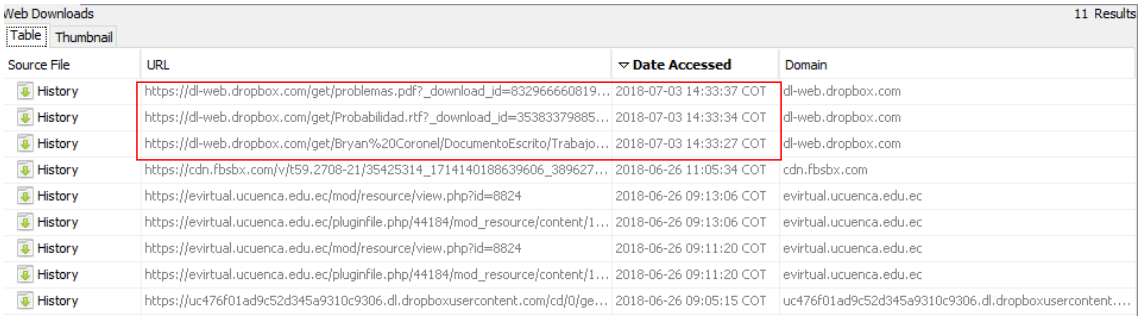


Figura 12: Descargas realizadas durante la realización de la prueba.

Como se aprecia en la metadata uno de los archivos descargados se denomina “Probabilidad.rtf” y fue almacenado en la carpeta de descargas, como se aprecia en la Figura 13.

Type	Value
URL	https://dl-web.dropbox.com/get/Probabilidad.rtf?_download_id=35383379885839616809363210663906418776384178490193600035941201329 4&_notify_domain=www.dropbox.com&_subject_uid=162488988&dl=1&revision_id=BHNn-NcwKHy8ngPgVr_ytHWEjlo-Z2SggIIBPapO2Rgj-tZelM3-26MF7jOWto5nOnTnORJ6eTdH9u-GmsHs2nH4GP8Z-e4Lkp8sfPURLcXldJdKqUptG9bDZdjbISXAHHY&w=AABENdkEmgEbFGnG9eEVeoh0G5OOaR1MI-5a3q5UunckVg
Domain	dl-web.dropbox.com
Program Name	Chrome
Path	C:\Users\Estudiante\Downloads\Probabilidad.rtf
Date Accessed	2018-07-03 14:33:34
Source File Path	/img_ImagenDataWeb001.vhd/vol_vol4/Drive-E_/PhysicalDrive0-1_/Users/Estudiante/AppData/Local/Google/Chrome/User Data/Default/History
Artifact ID	-9223372036854774508

Figura 13: metadatos del primer Ítem de descarga

En la memoria volátil se encontró que el archivo Probabilidad.rtf fue accedido, como se aprecia en la Figura 14.

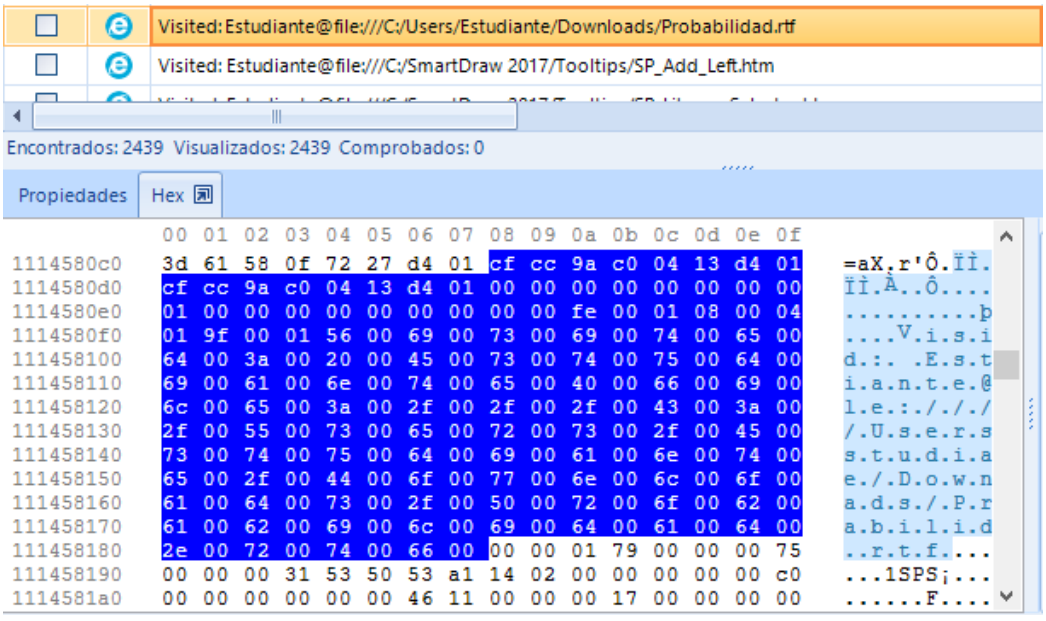


Figura 14: Registro de visita obtenido de la captura de memoria RAM.

De la misma forma analizando las URLs almacenadas en la memoria volátil, coinciden con los tres sitios web identificados: Facebook, Dropbox, Google y Evirtual, como se aprecia en la Figura 15.

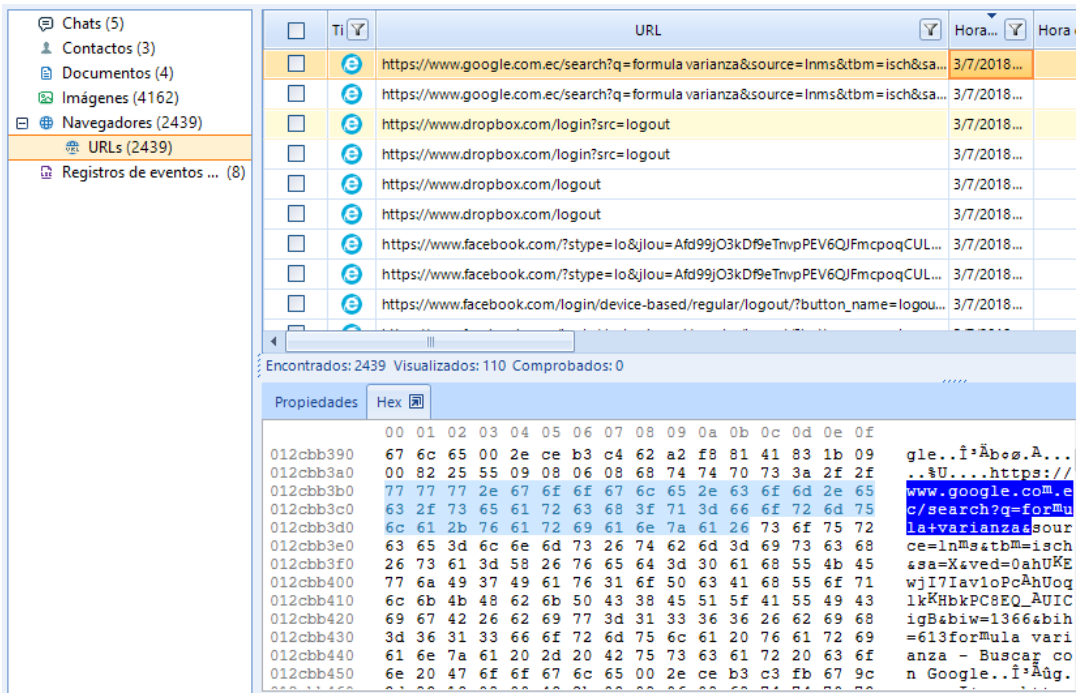


Figura 15: Registro de las URLs almacenadas en la captura de Memoria RAM.

6. INFORMACIÓN ADICIONAL

A. Caché Web

Al interactuar con aplicaciones dentro de entornos web, se realizan varias solicitudes de información por parte del cliente al servidor, para solucionar de alguna forma el problema de tener un número excesivo de peticiones, existe la memoria caché web. Es así como Castellano y Fanelli (2009), en su libro "Web Personalization in Intelligent Environments", establece que la caché web es "…un mecanismo desarrollado para reducir la latencia y el tráfico web." El mecanismo consiste en almacenar parte de las páginas web solicitadas por cierto periodo de tiempo (Castellano y Fanelli, 2009).

B. Cookies

Otro mecanismo empleado por los navegadores para reducir la latencia son las cookies. Las cookies en la web son pequeños archivos de texto creados por un sitio web y enviados al disco duro del ordenador del cliente (Tipton, 2014). Las cookies almacenan nuestras elecciones cada vez que se navega a través de Internet, para de manera posterior cuando una URL (Uniform Resource Locator) es escrita, el navegador web contacta el servidor y solicita el sitio web específico para ser desplegado en el monitor, pero además el navegador busca en el disco duro si existe alguna cookie procedente de este sitio; de ser el caso el navegador traslada la información en el archivo de vuelta al sitio (Tipton, 2014).

C. Archivos Temporales

Por lo general, además de las cookies o la caché web, los navegadores requieren en algunos casos mayor cantidad de información para cargar un sitio web; es ahí en donde los archivos temporales son necesarios. Un archivo temporal de Internet, de acuerdo a Koreneff y Sims-McLean (2005), es un archivo que se encuentra en el disco duro del usuario, en donde un navegador almacena información (como texto, imágenes, números) de un sitio web (Koreneff y Sims-McLean, 2005).

Es importante acotar, que la mayoría de navegadores permiten eliminar estos archivos del sistema (Koreneff y Sims-McLean, 2005). Otra información bastante útil que proporcionan los navegadores corresponde a sus historiales, pues por lo general un navegador almacena de acuerdo con EC- Council (2009 distintos historiales:

- *Historiales de Navegación*: Provee información de los sitios web visitados, estableciendo su URL y fecha de acceso.
- *Historiales de Descargas*: Por lo general contiene metadatos de los archivos descargados de la web, como fecha, directorio de descarga y el dominio del cual el archivo fue descargado.
- *Cuentas y Contraseñas Guardadas*: Algunos navegadores, con el fin de mejorar el servicio a sus usuarios proveen la opción de almacenar sus datos de acceso a sitios web, los cuales pueden ser visibles posteriormente.

7. DECLARACIÓN JURAMENTADA,

Yo Bryan Coronel. Declaro de manera voluntaria y bajo juramento que el informe que presento para dicha pericia es independiente y corresponde a mi real convicción profesional. Declaro también que toda la información aquí presente es verídica y llevada a cabo de manera rigurosa en los puntos pertinentes.

8. FIRMA Y RÚBRICA,

Perito: Bryan Daniel Coronel Tapia

CI: 010568208 – 2

Anexo C: Artículo publicado

A Systematic Literature Review in Cyber Forensics: Current Trends from the Client Perspective

***Abstract*— Nowadays, with the demand of web applications there is also an increase in the number of problems and crimes that demand an investigation that requires digital forensics techniques in order to manage web evidence. Although there are several studies that address cyber forensics, they are mainly oriented to manage evidence at server side, as far as we know, no systematic literature reviews have been reported on how cyber forensics is addressed at clients' side; considering the internationals standards. Thus, this paper reports a literature review about how cyber forensics is addressed at clients' side related to techniques of identification, collection, analysis, preservation and report of digital evidence. Also, a review of how standards are being used in cyber forensics focused on the client side. The aim of this study is to provide a background of relevant activities that are considered by investigators to handle with potentially digital evidence from web environments, considering what internationals standards are solving for this purpose. Thus, a total of 37 studies have been selected and analyzed in this study. Moreover, this study provides important insights about the need to create methodologies aligned with formal standards that support the management of the evidence in an appropriate way.**

Keywords*— *digital evidence, cyber forensics, client side, systematic review, standards

I. Introduction

Currently, web applications have been adopted in the most of transactional systems of organizations. Also, there are applications deployed on web environments for different purposes (e.g., social networks, email, cloud storage). With the mass use of online applications, there is also an increase in the number of crimes, cyber-attacks, and punishable by law activities [1]. In general, people use web browsers or desktop applications that request pages and resources to a server; therefore, it is important to manage digital evidence left in client's computers by using suitable forensics guidelines [2].

Moreover, with the emergence of new web technologies and cloud computing with their service models (i.e., Infrastructure as a Service, Platform as a Service and Software as a Service) [3] the importance of digital evidence has increased substantially [4]. Also, there are studies that consider the current increase in the number of applications deployed on the cloud, several authors address their studies in a similar way to both web and SaaS (Software as a Service) applications at client's side [5], [6], because in both cases forensics investigators do not have access to the server.

Then, a literature review is a way to identify, evaluate, and interpret all available research relevant to a particular topic area, or phenomenon of interest [7]. There are studies that provide systematic reviews or mappings about cyber forensics and the managing of digital evidence [8]–[10]. Thus, Guo et al., [8] provide concepts, principles, and a process for performing a forensic investigation; however, they do not cover cyber forensics and it specific considerations at client's side. In addition, Hatole y Bawiskar [9] present a literature review about email forensics, they also present techniques and tools; however, this study addresses a forensics process only for emails. Finally, Kaur et al. [10] propose a literature review on cyber forensics and its analysis tools; however, they are focused on general aspects without taking into account the client perspective and the classification of the evidence that investigators can find.

Consequently, this paper presents a secondary study about cyber forensics with guidelines that support the forensics management from web environments focused on the client-side. Also, it analyses the standards that can be useful for forensics investigations, and there are: (i) ISO/IEC 27037, which reviews guidelines for identification, collection, acquisition, and preservation of the digital evidence [11]; (ii) ISO/IEC 27042 that provides guidelines for the analysis and interpretation of digital evidence [12]; (iii) ISO/IEC 27041 that provides guidance on assuring suitability and adequacy of incident investigative method [13]; (iv) ISO/IEC 27017, which is a code of practice for information security controls based on ISO/IEC 27002 but can be used specifically for cloud services [14]; and finally, (v) ISO/IEC 27050 that provides requirements and guidance on activities in electronic discovery [15]. The result of this systematic review is an overview of current research studies related to cyber forensics in order to manage digital evidence from web environments at the client side.

Finally, this paper is structured as follows: Section 2 presents an overview of the state of the research related to web forensics at client's side. In Section 3 it is described the research method that is used to identify the relevant literature related to this contribution. Section 4 presents the results of the research method and describes the relevant approaches according to the mentioned classification. Section 5 presents a discussion of the results obtained by the followed methodology according to the literature. Finally, the conclusions are presented in Section 6.

II. Related work

There are some secondary studies related to guidelines to manage digital evidence from web environments [8]–[10], [16]–[18]. Therefore, Guo et al. [8] present some definitions and principles related to computer forensics and digital evidence; however, the authors study the digital evidence in a general way, without specifically considering obtaining evidence on the client's side. On the other hand, Garfinkel [17] presents a literature review where the author addresses the problems of current forensics processes and challenges in the near future; however, the author does not cover digital evidence from web environments. Simou et al. [16] address a review of cloud forensics; the authors are focused on available technical solutions presented in primary studies that have applicability on cloud computing specifically the SaaS service model; and provide general guidelines to be considered respected to artifacts in that service model.

Anexo D: Artículo publicado 2.

Forensics Analysis on Mobile Devices: A Systematic Mapping Study

Abstract. Nowadays, mobile devices have evolved vertiginously due to their massive adoption by users, who have several devices with different purposes. These devices contain greater capacity / functionality to manage information, with the embedded characteristics they become an important digital evidence container. In recent years, considerable research has been conducted on various digital electronic evidence, acquisition schemes and methods of extracting evidence from mobile devices. In this paper, a systematic mapping of the Forensics Analysis on Mobile Device is presented, this research has been conducted following the guidelines of Kitchenham's methodology. The aim of this study is to provide a background of relevant activities that are considered by investigators to handle with potentially digital evidence from mobile devices. A total of 36 primary studies were selected and categorized to extract information regarding the aforementioned classification. The results presented in this contribution provide a detailed study about current analysis in research forensics field by using mobile devices.

Keywords: Forensics; Digital Evidence; Devices.

1 Introduction

Nowadays, mobile devices are being used massively, becoming one of the best inventions that have existed, mainly because of their functionality, contents, and versatility. Smartphones are mini computers that provide the functionality of conventional telephones, wireless Internet access, and, recently, many booming applications. They also provide sources of information in real time, exchange of data and information on a daily basis. Besides, they represent an interesting source of proof for crime research due to the content that can be found stored on one of those devices (e.g., bank transactions, social interaction). Fraudsters and other cyber criminals can use different services provided by platforms with false identities, in order to hide their malicious intentions behind profiles that seem to be reliable.

The digital forensic analysis has been defined as the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation and presentation of digital evidence [S09]. The challenge of preserving and managing the evidence existing in mobile devices has motivated the creation of methods and solutions to manage the evidence in a properly way.

As far as it is known, no evidence-based studies (e.g., systematic mapping studies, systematic literature reviews) have been recently reported about the considerations with which forensic tools perform treatment of electronic digital evidence into mobile devices. A systematic mapping study is a way to categorize and summarize the existing information around a research question in an unbiased manner [6]. Therefore, a